

日 本 国 特 許 庁
JAPAN PATENT OFFICE

S. Arita
8/20/03
Q76964
10f1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 8 月 2 1 日
Date of Application:

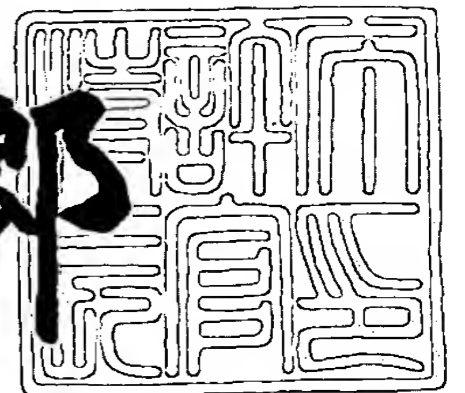
出 願 番 号 特 願 2 0 0 2 - 2 4 0 0 3 4
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 4 0 0 3 4]

出 願 人 日 本 電 気 株 式 会 社
Applicant(s):

2 0 0 3 年 7 月 9 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太 田 信 一 郎



出 証 番 号 出 証 特 2 0 0 3 - 3 0 5 5 3 1 2

【書類名】 特許願

【整理番号】 35001156

【提出日】 平成14年 8月21日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 有田 正剛

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088812

 【弁理士】

 【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

 【予納台帳番号】 030982

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9001833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ヤコビ群要素加算装置

【特許請求の範囲】

【請求項 1】 有限体上定義された、

$$Y^3 + \alpha_0 X^4 + \alpha_1 XY^2 + \alpha_2 X^2 Y + \alpha_3 X^3 + \alpha_4 Y^2 + \alpha_5 XY + \alpha_6 X^2 + \alpha_7 Y + \alpha_8 X + \alpha_9$$

もしくは、

$$Y^2 + \alpha_0 X^5 + \alpha_1 X^2 Y + \alpha_2 X^4 + \alpha_3 X Y + \alpha_4 X^3 + \alpha_5 Y + \alpha_6 X^2 + \alpha_7 X + \alpha_8$$

もしくは、

$$Y^2 + \alpha_0 X^7 + \alpha_1 X^3 Y + \alpha_2 X^6 + \alpha_3 X^2 Y + \alpha_4 X^5 + \alpha_5 X Y + \alpha_6 X^4 + \alpha_7 Y + \alpha_8 X^3 + \alpha_9 X^2 + \alpha_{10} X + \alpha_{11}$$

なる多項式で定義された代数曲線のヤコビ群における加算を実行する演算装置であって、

前記代数曲線を表すパラメータとして定義体位数、単項式順序、係数リストを記述した代数曲線パラメータファイルを入力する手段と、

前記ヤコビ群の要素を表す、前記代数曲線パラメータファイルで指定された代数曲線の座標環のイデアルのグレブナ基底 I_1 および I_2 を入力する手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 I_1 が生成するイデアルとグレブナ基底 I_2 の生成するイデアルとのイデアル積のグレブナ基底 J を演算するイデアル合成手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 J が生成するイデアルの逆イデアルと同値なイデアルのうち前記代数曲線パラメータファイルで指定された単項式順序において最小のイデアルのグレブナ基底 J^* を演算する第一のイデアル縮約手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 J^* が生成するイデアルの逆イデアルと同値なイデアルのうち前記代数曲線パラメータファイルで指定された単項式順序において最小のイデアルのグレブ

ナ基底 J^{**} を演算して出力する第二のイデアル縮約手段と、
 を備えたことを特徴とするヤコビ群要素加算装置。

【請求項 2】 前記イデアル合成手段は、

入力された複数のベクトル v_1, v_2, \dots, v_n に対して、掃き出し法を用いて、その全ての1次独立な線形従属関係 $\sum_j m_{j,i} v_j = 0$ ($j=1, 2, \dots$)を表す複数のベクトル $m_1=(m_{1,1}, m_{1,2}, \dots, m_{1,n}), m_2=(m_{2,1}, m_{2,2}, \dots, m_{2,n}), \dots$ を出力する線形関係導出手段と、

レコード番号フィールド、イデアル型番号フィールド、位数フィールドおよびイデアル型フィールドからなるイデアル型テーブルと、

レコード番号フィールド、位数フィールドおよび単項式リストフィールドからなる単項式リストテーブルと、

レコード番号フィールド、位数フィールド、成分番号リストフィールド、第一ベクトル型フィールド、第二ベクトル型フィールドおよび第三ベクトル型フィールドからなるグレブナ基底構成用テーブルと、

前記代数曲線パラメータファイルを取得し、入力されたグレブナ基底 I_1 および I_2 それぞれに対して、前記イデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル I_i ($i=1, 2$)の型と一致するレコードを検索し、検索されたレコードのイデアル型番号フィールドの値 N_i および位数フィールドの値 d_i を取得するイデアル型分類手段と、

前記位数フィールドの値 d_1 および d_2 の和 $d_3=d_1+d_2$ を計算し、単項式リストテーブルを参照し前記 d_3 を位数フィールドの値に持つレコード R を検索し、前記レコード R の単項式リストフィールドに記述されている単項式のリスト M_1, M_2, \dots を取得し、 I_1 と I_2 が異なるときには、前記各単項式 M_i を I_1 で割った剰余式 r_i を計算し、前記代数曲線パラメータファイルに記述された単項式順序に従って剰余式 r_i の係数からなるベクトル $w^{(i)}_1$ を生成し、さらに、 M_i を I_2 で割った剰余式 s_i を計算し、代数曲線パラメータファイル A に記述された単項式順序に従って剰余式 s_i の係数からなるベクトル $w^{(i)}_2$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル v_i を生成し、また、 I_1 と I_2 が等しいときには、前記各単項式 M_i を I_1 で割った剰余式 r_i を計算し、前記代数曲線パラメータファイルに記述された単項式順

序に従って剰余式 r_i の係数からなるベクトル $w^{(i)}_1$ を生成し、さらに、前記代数曲線パラメータファイルに記述された係数リストおよび単項式順序を用いて定義多項式 F を構成し、多項式 M に対してその X による微分を $D_X(M)$ 、 Y による微分を $D_Y(M)$ と書くとき、多項式 $D_X(M_i) D_Y(F) - D_Y(M_i) D_X(F)$ を I_1 で割った剰余式 s_i を計算し、前記代数曲線パラメータファイルに記述された単項式順序に従って剰余式 s_i の係数から成るベクトル $w^{(i)}_2$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル v_i を生成する単項式ベクトル生成手段と、

前記複数のベクトル v_1, v_2, \dots を前記線形関係導出装置に入力し、出力として複数のベクトル m_1, m_2, \dots を得て、前記グレブナ基底構成用テーブルを参照し前記値 d_3 を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル m_1, m_2, \dots 中に存在しないレコード R_2 を検索し、前記複数のベクトル m_1, m_2, \dots 中から、前記レコード R_2 の第一ベクトル型に一致するベクトル m を選択し、前記代数曲線パラメータファイルに記述された単項式順序に従ってベクトル m の成分の値を係数とする多項式 f_1 を生成し、以下、同様にして、第二ベクトル型に一致するベクトルを用いて多項式 f_2 を、また第三ベクトル型に一致するベクトルを用いて多項式 f_3 を生成し、多項式の集合 $J = \{f_1, f_2, f_3\}$ を得て、前記グレブナ基底 J として出力する基底構成手段とを有することを特徴とする請求項1記載のヤコビ群要素加算装置。

【請求項3】 前記第一および第二のイデアル縮約手段の各々は、
入力された複数のベクトル v_1, v_2, \dots, v_n に対して、掃き出し法を用いて、その全ての1次独立な線形従属関係 $\sum_j m_{j,i} v_i = 0$ ($j=1, 2, \dots$)を表す複数のベクトル $\{m_1=(m_{1,1}, m_{1,2}, \dots, m_{1,n}), m_2=(m_{2,1}, m_{2,2}, \dots, m_{2,n}), \dots\}$ を出力する線形関係導出手段と、

レコード番号フィールド、イデアル型番号フィールド、縮約位数フィールド、およびイデアル型フィールドからなるイデアル型テーブルと、

レコード番号フィールド、位数フィールドおよび単項式リストフィールドからなる単項式リストテーブルと、

レコード番号フィールド、位数フィールド、成分番号リストフィールド、第一ベ

クトル型フィールド、第二ベクトル型フィールドおよび第三ベクトル型フィールドからなるグレブナ基底構成用テーブルと、

前記代数曲線パラメータファイルを取得し、前記イデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアルJの型と一致するレコードを検索し、検索されたレコードのイデアル型番号フィールドの値Nおよび縮約位数フィールドの値dを取得するイデアル型分類手段と、

前記dが0であるときには、入力イデアルJを前記グレブナ基底 J^* として出力し、

前記dが0でないときには、前記単項式リストテーブルを参照し前記dを位数フィールドの値に持つレコードRを検索し、前記レコードRの単項式リストフィールドに記述されている単項式のリスト M_1, M_2, \dots を取得し、前記代数曲線パラメータファイルに記述された係数リストおよび単項式順序を用いて定義多項式Fを構成し、入力イデアルJの第一番目の多項式f、第二番目の多項式gおよび第三番目の多項式hを取得し、前記各単項式 M_i と多項式gの積 $M_i \cdot g$ の、多項式fおよびFによる剰余式 r_i を計算し、前記代数曲線パラメータファイルに記述された単項式順序に従って剰余式 r_i の係数からなるベクトル $w^{(i)}_1$ を生成し、さらに、前記各単項式 M_i と多項式hの積 $M_i \cdot h$ の、多項式fおよびFによる剰余式 s_i を計算し、前記代数曲線パラメータファイルに記述された単項式順序に従って剰余式 s_i の係数からなるベクトル $w^{(i)}_2$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル v_i を生成する多項式ベクトル生成手段と、

前記複数のベクトル v_1, v_2, \dots を前記線形関係導出手段に入力し、出力として複数のベクトル m_1, m_2, \dots を得て、前記グレブナ基底構成用テーブルを参照して前記値dを位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル m_1, m_2, \dots 中に存在しないレコード R_2 を検索し、前記複数のベクトル m_1, m_2, \dots の中から、前記レコード R_2 の第一ベクトル型に一致するベクトルmを選択し、ベクトルmの成分の値を係数とする多項式 f_1 を前記代数曲線パラメータファイルに記述された単項式順序に従って生成し、以下、同様にして、第二ベクトル型に一致するベクトルを用いて多項式 f_2 を生成し、また第三ベクトル型に一致するベクトルを用いて多項式 f_3 を生成し、多項式の集合 $\{f_1, f_2, f_3\}$ を得て、前記グレ

ブナ基底 J^* もしくは J^{**} として出力する基底構成手段とを有することを特徴とする請求項1または2記載のヤコビ群要素加算装置。

【発明の詳細な説明】

【0 0 0 1】

【産業上の利用分野】

本発明はヤコビ群要素加算装置に関し、特に情報セキュリティ技術としての暗号技術である離散対数型暗号の一種である代数曲線のヤコビ群を用いた離散対数型暗号(以下、代数曲線暗号と呼ぶ)技術に関するものである。

【0 0 0 2】

【従来の技術】

代数曲線暗号の中で、最も実用化が進んでいるのは、楕円曲線暗号である。しかし、楕円曲線暗号で用いられる楕円曲線は一般の代数曲線に比べて非常に特殊な曲線である。その特殊性を用いた攻撃法が将来発見される危険がある。そのため、より安全性を確保するためには、より特殊性の低い、一般的な代数曲線を用いることが望ましい。そのような、より一般的な代数曲線を用いることができる代数曲線暗号として C_{ab} 曲線暗号が知られている。

【0 0 0 3】

しかしながら、楕円曲線暗号にくらべ C_{ab} 曲線暗号は産業界で用いられていない。その大きな理由は、有田 正剛著、 C_{ab} 曲線のヤコビアン群加算アルゴリズムとその離散対数型暗号への応用、電子情報通信学会和文論文誌、J82-A巻、8号、1291--1299、1999に示されている、従来の C_{ab} 曲線のヤコビ群における加算アルゴリズムが楕円曲線のヤコビ群における加算アルゴリズムに比べ、数十倍程度遅いため、 C_{ab} 曲線暗号では、楕円曲線暗号にくらべ、暗号化復号化の処理効率が著しく悪いためである。

【0 0 0 4】

また、原澤 隆一、鈴木 譲著、ア・ファースト・ヤコビアン・グループ・アリスメティック・スキーム・フォー・アルジェブレイク・カーブ・クリプトグラフィ、E84-A巻、1号、pp.130-139、2001 (Ryuichi HARASAWA, Joe SUZUKI, A Fast Jacobian Group Arithmetic Scheme for Algebraic Curve Cryptography, Vol.E84

-A.No.1, pp.130-139, 2001)においても、 C_{ab} 曲線のヤコビ群における加算アルゴリズムが提案されているが、アルゴリズムの漸近的な計算量は与えられているものの、実装実験における実行速度データは示されておらず、また他者による実装実験の報告もなく、現実的にどの程度の実行速度が得られるか不明である。

【 0 0 0 5 】

【発明が解決しようとする課題】

上に見たように、 C_{ab} 曲線のヤコビ群における加算アルゴリズムの非効率さが当該曲線の暗号の実用化を阻んでおり、よって C_{ab} 曲線のヤコビ群における加算アルゴリズムを高速化することが要求されている。

本発明はかかる要求に鑑みてなされたものであつて、その目的とするところは、 C_{ab} 曲線のヤコビ群における加算アルゴリズムを高速化することが可能なヤコビ群要素加算装置を提供することにある。

【 0 0 0 6 】

【課題を解決するための手段】

本発明によるヤコビ群要素加算装置は、有限体上定義された、

$$Y^3 + \alpha_0 X^4 + \alpha_1 XY^2 + \alpha_2 X^2 Y + \alpha_3 X^3 + \alpha_4 Y^2 + \alpha_5 XY + \alpha_6 X^2 + \alpha_7 Y + \alpha_8 X + \alpha_9$$

もしくは、

$$Y^2 + \alpha_0 X^5 + \alpha_1 X^2 Y + \alpha_2 X^4 + \alpha_3 X Y + \alpha_4 X^3 + \alpha_5 Y + \alpha_6 X^2 + \alpha_7 X + \alpha_8$$

もしくは、

$$Y^2 + \alpha_0 X^7 + \alpha_1 X^3 Y + \alpha_2 X^6 + \alpha_3 X^2 Y + \alpha_4 X^5 + \alpha_5 X Y + \alpha_6 X^4 + \alpha_7 Y + \alpha_8 X^3 + \alpha_9 X^2 + \alpha_{10} X + \alpha_{11}$$

なる多項式で定義された代数曲線のヤコビ群における加算を実行する演算装置であつて、

前記代数曲線を表すパラメータとして定義体位数、単項式順序、係数リストを記述した代数曲線パラメータファイルを入力する手段と、

前記ヤコビ群の要素を表す、前記代数曲線パラメータファイルで指定された代数曲線の座標環のイデアルのグレブナ基底 I_1 および I_2 を入力する手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 I_1 が生成するイデアルとグレブナ基底 I_2 の生成するイデアルとのイデアル積のグレブナ基底 J を演算するイデアル合成手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 J が生成するイデアルの逆イデアルと同値なイデアルのうち前記代数曲線パラメータファイルで指定された単項式順序において最小のイデアルのグレブナ基底 J^* を演算する第一のイデアル縮約手段と、

前記代数曲線パラメータファイルで指定された代数曲線の座標環における、グレブナ基底 J^* が生成するイデアルの逆イデアルと同値なイデアルのうち前記代数曲線パラメータファイルで指定された単項式順序において最小のイデアルのグレブナ基底 J^{**} を演算して出力する第二のイデアル縮約手段と、
を備えたことを特徴とする。

【 0 0 0 7 】

【作用と原理】

[C_{ab} 曲線とそのヤコビ群]

本発明で扱う、 C_{ab} 曲線 C は、互いに素な 2 つの自然数 a と b に対して、以下の形の多項式 $F(X, Y)$ によって定義される非特異な平面曲線である。

$$F(X, Y) = Y^a + c_0 X^b + \sum c_{i,j} X^i Y^j.$$

ただし、上式で添数 i, j は0以上の自然数で $a i + b j < ab$ の範囲を動く。また、 $c_0, c_{i,j}$ は定義体 k の元で、 c_0 は0ではないとする。 C_{ab} 曲線 C は唯一の無限遠点 P_∞ をもち、多項式 Y と X はそれぞれ P_∞ で b 位と a 位の唯一の極をもつ。 C_{ab} 曲線 C 上の次数0の因子のなす群を $D_C^0(k)$ とおき、主因子のなす群を $P_C(k)$ とおく。

【 0 0 0 8 】

本発明でその加算アルゴリズムを求めたいヤコビ群 $J_C(k)$ は、

$$J_C(k) = D_C^0(k) / P_C(k)$$

と定義される。一方、 $R=k[X, Y]/F$ を C_{ab} 曲線 C の座標環とすると、定義より C_{ab} 曲線 C は非特異なので、環 R は整閉整域となり、Dedekind domainである。よって、環 R の0でない分数イデアル全体は群 $I_R(k)$ をなす。環 R の主イデアルのなす群を $P_R(k)$ とおくと、環 R のイデアル類群 $H_R(k)$ が、

$$H_R(k) = I_R(k) / P_R(k)$$

と定義される。

【 0 0 0 9 】

一般に、非特異な代数曲線に対して、曲線上の因子と座標環のイデアルとは同一視することができ、そのヤコビ群とイデアル類群は自然に同型であることが知られている。特に、 C_{ab} 曲線 C のヤコビ群 $J_C(k)$ は座標環 R のイデアル類群 $H_R(k)$ と自然に同型である。アルゴリズムの実装には因子よりもイデアルが便利なので、以下 C_{ab} 曲線 C のヤコビ群 $J_C(k)$ は座標環 R のイデアル類群 $H_R(k)$ として扱う。

【 0 0 1 0 】

[グレブナ基底に関する準備]

イデアル類群 $H_R(k)$ を対象とした計算ではイデアルのグレブナ基底を用いるので、本節ではそれに関する準備を行う。一般に、多項式環 $S = k[X_1, \dots, X_n]$ に対して、その単項式の間の順序 ' $<$ ' であって、積とコンパチブル、すなわち $M_1 < M_2$ ならば、常に $M_1 M_3 < M_2 M_3$ となる整列順序 ' $<$ ' を単項式順序と呼ぶ。本節では以降、多項式環 S に対し、任意の単項式順序 ' $<$ ' が与えられているとする。

S の多項式 f に対して、 f に現れる、単項式順序 ' $<$ ' に関する最大の単項式を f の leading monomial と呼び、 $LM(f)$ とかく。また、イデアル I に対して、 I に属する多項式の leading monomial 全体が生成するイデアルを $LM(I)$ と書く。

【 0 0 1 1 】

多項式 f_1, \dots, f_s で生成される、 S のイデアル $I = (f_1, \dots, f_s)$ に対して、 $\{f_1, \dots, f_s\}$ が

$LM(I) = (LM(f_1), \dots, LM(f_s))$ を満たすとき、 $\{f_1, \dots, f_s\}$ はイデアル I のグレブナ基底と呼ばれる。多項式環 S のイデアル I に対し、 $LM(I)$ に属さない単項式(あるいはその multi degree)全体 $\Delta(I)$ は I のデルタ集合と呼ばれる。 $\Delta(I)$ に含まれる各単項式(の multi-degree)をプロットすると、凸集合が現れ、その凸集合を囲む格子点が I のグレブナ基底の要素の leading monomial と対応する。また、 $\Delta(I)$ は k 上のベクトル空間 S/I の基底をなす。

【 0 0 1 2 】

非特異アフィン代数曲線 C の座標環 $R = S/F$ のイデアル I は、多項式環 S のイデアルで

、曲線Cの定義イデアルFを含むものと同一視できる。よって、座標環Rのイデアルに対しても、上のようにグレブナ基底を考えることができる。座標環 $R=S/F$ の0次元イデアルI(すなわち、Iの解集合が有限集合)に対して、 k 上のベクトル空間 S/I の次元をイデアルIの位数と呼び、 $\delta(I)$ と書く。定義より直ちに、 $\delta(I)$ は集合 $\Delta(I)$ の位数に等しい。また、非特異性の仮定より、 $\delta(IJ)=\delta(I)\delta(J)$ となる。 $I=(f)$ がRの主イデアルのときは、 $\delta(I) = -vp_{\infty}(f)$ である。ここで、 $vp_{\infty}(f)$ は多項式 f の P_{∞} での付値を表す。

【 0 0 1 3 】

[C_{ab} 曲線のヤコビ群加算アルゴリズム その1]

多項式 $F(X,Y)$ で定義された C_{ab} 曲線Cの座標環 $R=k[X,Y]/F$ を考える。2変数単項式 $X^m Y^n$ を曲線C上の関数と見なし、 P_{∞} における極位数 $-v_{P_{\infty}}(X^m Y^n)$ の大小によって単項式を順序づけた単項式順序を C_{ab} 順序と呼ぶ。ただし、 P_{∞} における極位数が等しいときは、 Y の次数が大きい方を大とする。以下、 C_{ab} 曲線Cの座標環Rの単項式順序として C_{ab} 順序を用いる。座標環RのイデアルIに対し、Iに含まれる0でない多項式でそのleading monomialが C_{ab} 順序で最小である多項式を f_I とかく。さらに、 $I^* = (f_I) : I (= \{ g \in R \mid g \cdot I \subseteq (f_I) \})$ とおく。

【 0 0 1 4 】

このとき、 I, J を座標環Rの任意の(整)イデアルとすると、(1) I と I^{**} は同値であり、(2) I^{**} は I と同値な(整)イデアルでその位数が最小のものであり、(3) I と J が同値ならば $I^*=J^*$ であり、とくに、 $I^{**}=(I^{**})^{**}$ である、ことが容易にわかる。座標環RのイデアルIに対して、 $I^{**}=I$ であるとき、 I をreduced idealと呼ぶ。上記(1), (3)より、任意のイデアルは唯一のreduced idealに同値である。すなわち、reduced ideal はイデアル類の代表系をなしている。この性質は C_{ab} 順序に限らず、任意の単項式順序を用いた場合にも成立するが、 C_{ab} 順序を用いた場合は、上記(2)より、reduced ideal はそれと同値なイデアルのうち、位数が最小のものとなるという特質を持つ。これは、アルゴリズムの実装に際して利点となる。reduce ideal をイデアル類の代表系として用いて、以下のイデアル類群乗算＝ヤコビ群加算アルゴリズムを得る。

【 0 0 1 5 】

[ヤコビ群加算アルゴリズム 1]

入力：座標環 R のreduced ideals I_1, I_2 出力：イデアル積 $I_1 \cdot I_2$ に同値な reduced ideal I_3

1. $J \leftarrow I_1 \cdot I_2$
2. $J^* \leftarrow (f_J) : J$
3. $I_3 \leftarrow (f_{J^*}) : J^*$

【 0 0 1 6 】

[イデアルの分類]

上記ヤコビ群加算アルゴリズム 1 を効率的でかつ実装しやすいプログラムとして実現するために、ヤコビ群加算アルゴリズム 1 の実行中に現れるイデアルを分類する。以下、簡単のため、 C_{34} 曲線(すなわち、 $a=3, b=4$ とした C_{ab} 曲線)を対象として説明するが、一般の C_{ab} 曲線に対しても同様である。 C_{34} 曲線の種数は3なので、ヤコビ群加算アルゴリズム 1 の実行中に現れるイデアルの位数は6以下である。それらの C_{34} 順序におけるグレブナ基底は位数ごとに以下のように分類される。ただし、以降、イデアルのグレブナ基底に C_{34} 曲線 C の定義式 F が現れても、 F は省略して書かない。また、グレブナ基底を構成する各多項式の係数 a_i, b_j, c_k は全て k の元である。

【 0 0 1 7 】

(位数6のイデアル)

I を座標環 R の位数6のイデアルとする。位数の定義より、 $V=R/I$ は定義体 k 上の6次元ベクトル空間である。イデアル I が表す6点が「一般的な」位置にあるとき、 C_{34} 順序で最初から6つの単項式 $1, X, Y, X^2, X Y, Y^2$ はそれら6点上で1次独立である。すなわち、単項式 $1, X, Y, X^2, X Y, Y^2$ はベクトル空間 V の基底をなす。このとき、イデアル I をタイプ61のイデアルと呼ぶ。

【 0 0 1 8 】

一般に、イデアル I のデルタ集合 $\Delta(I)$ はベクトル空間 V の基底と同一視できるので、タイプ61のイデアル I のデルタ集合は

$$\Delta(I) = \{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2)\}$$

となる。それらを囲む格子点集合は $\{(0, 3), (1, 2), (2, 1), (3, 0)\}$ である。よって、タイプ61のイデアルIのグレブナ基底は以下の形をもつ。

$$\begin{aligned} \text{タイプ61のイデアルのグレブナ基底} = & \{ X^3 + a_6 Y^2 + a_5 X Y + a_4 X^2 + a_3 Y \\ & + a_2 X + a_1, \\ & X^2 Y + b_6 Y^2 + b_5 X Y + b_4 X^2 + b_3 Y + b_2 X + b_1, \\ & X Y^2 + c_6 Y^2 + c_5 X Y + c_4 X^2 + c_3 Y + c_2 X + c_1 \} \end{aligned}$$

これら3式はそれぞれ格子点 $(3, 0)$, $(2, 1)$, $(1, 2)$ に対応する (格子点 $(0, 3)$ は定義式Fに対応)。一般には、6つの単項式 $1, X, Y, X^2, X Y, Y^2$ は、イデアルIが表す6点上で、すなわちベクトル空間Vにおいて一次独立とは限らない。

【 0 0 1 9 】

まず、Vにおいて、 C_{34} 順序で最初から5つの単項式 $1, X, Y, X^2, X Y$ が一次独立であり、6番目の単項式 Y^2 がそれらの線形結合で表される場合を考察する。仮定より、 $\Delta(I)$ は $\{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1)\}$ を含み、 $(2, 0)$ を含まない位数6の凸集合である。よって、 $\Delta(I) = \{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (2, 1)\}$ であるか $\Delta(I) = \{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (3, 0)\}$ であるかのいずれとなる。 $\Delta(I)$ が前者のとき、Iをタイプ62のイデアルと呼び、後者の場合、Iをタイプ63のイデアルと呼ぶ。

$\Delta(I)$ を囲む格子点集合は、タイプ62のとき $\{(0, 2), (3, 0)\}$ であり、タイプ63のとき $\{(0, 2), (2, 1), (4, 0)\}$ である。よって、グレブナ基底は以下のようになる。

$$\begin{aligned} \text{タイプ62のイデアルのグレブナ基底} = & \{ Y^2 + a_5 X Y + a_4 X^2 + a_3 Y + a_2 X + \\ & a_1, \\ & X^3 + b_5 X Y + b_4 X^2 + b_3 Y + b_2 X + b_1 \} \end{aligned}$$

これら2式はそれぞれ格子点 $(0, 2)$, $(3, 0)$ に対応する。

【 0 0 2 0 】

$$\begin{aligned} \text{タイプ63のイデアルのグレブナ基底} = & \{ Y^2 + a_5 X Y + a_4 X^2 + a_3 Y + a_2 X \\ & + a_1, \end{aligned}$$

$$X^2 Y + b_6 X^3 + b_5 X Y + b_4 X^2 + b_3 Y + b_2 X + b_1 \}$$

これら2式はそれぞれ格子点 $(0, 2)$, $(2, 1)$ に対応する。

ただし、タイプ63のイデアルのグレブナ基底には本来、格子点 $(4, 0)$ に対応する

多項式が存在するが、定義式Fと格子点(0, 2)に対応する式 $f=Y^2 + a_5 X Y + a_4 X^2 + a_3 Y + a_2 X + a_1$ から、 $F - Y f$ と、ただちに計算できるので、省略している。

【 0 0 2 1 】

次に、Vにおいて、最初から4つの単項式1, X, Y, X^2 が一次独立であり、5番目の単項式 $X Y$ がそれらの線形結合で表されたとする。すなわち、 $\Delta(I)$ は $\{(0, 0), (1, 0), (0, 1), (2, 0)\}$ を含み、 $(1, 1)$ を含まない。このとき、 $\Delta(I)$ が(0, 2)を含まないと仮定すると、 $\Delta(I)$ が位数6をもつには、

$$\Delta(I) = \{(0, 0), (1, 0), (0, 1), (2, 0), (3, 0), (4, 0)\}$$

となるしかない。ところが、仮定より、Iはleading termが Y^2 である多項式 $f=Y^2 + \dots$ を含む。すると $Y f - F = X^4 + \dots$ がIに属するので、 $(4, 0)$ は $\Delta(I)$ には属さない。これは矛盾である。以上より、 $\Delta(I)$ は必ず(0, 2)を含むことがわかり、 $\Delta(I) = \{(0, 0), (1, 0), (0, 1), (2, 0), (0, 2), (3, 0)\}$ となる。このときIをタイプ64のイデアルとよぶ。

【 0 0 2 2 】

タイプ64のイデアルIのデルタ集合 $\Delta(I)$ を囲む格子点集合は $\{(0, 3), (1, 1), (4, 0)\}$ である。よって、タイプ64のイデアルIのグレブナ基底は以下になる。

$$\text{タイプ64のイデアルのグレブナ基底} = \{X Y + a_4 X^2 + a_3 Y + a_2 X + a_1, X^4 + b_6 X^3 + b_5 Y^2 + b_4 X^2 + b_3 Y + b_2 X + b_1\}$$

これら2式はそれぞれ格子点(1, 1), (4, 0)に対応する(格子点(0, 3)は定義式Fに対応)。

【 0 0 2 3 】

次に、 $V=R/I$ において、 C_{34} 順序で最初から3つの単項式1, X, Yが一次独立であり、4番目の単項式 X^2 がそれらの線形結合で表されたとする。このとき、イデアルIには X^2 をleading termとする多項式fが含まれ、デルタ集合は、

$$\Delta(I) = \{(0, 0), (1, 0), (0, 1), (1, 1), (0, 2), (1, 2)\}$$

となり、それらを囲む格子点集合は $\{(0, 3), (2, 0)\}$ となるので、Iはfで生成される単項イデアルとなる。このとき、Iをタイプ65のイデアルと呼ぶ。

$$\text{タイプ65のイデアルのグレブナ基底} = \{X^2 + a_3 Y + a_2 X + a_1\}$$

上式は格子点(2, 0)に対応する(格子点(0, 3)は定義式Fに対応)。

【 0 0 2 4 】

Y(以下の項)をleading termとする多項式fは $\deg((f)_0) = -v_{p_\infty}(f)=4 < 6$ より、位数6のイデアルIに対応する6点で同時に消えることはない。よって、 $V=R/I$ において最初から3つの単項式1, X, Yは必ず一次独立であり、以上で位数6のイデアルの分類は完了した。

【 0 0 2 5 】

(位数5のイデアル)

Iを座標環Rの位数5のイデアルとする。位数5のイデアルも位数6のイデアルと同様にして、以下のようにタイプ51からタイプ54に分類される。

タイプ51のイデアルのグレブナ基底 = $\{ Y^2 + a_5 X Y + a_4 X^2 + a_3 Y + a_2 X + a_1,$

$X^3 + b_5 X Y + b_4 X^2 + b_3 Y + b_2 X + b_1,$

$X^2 Y + c_5 X Y + c_4 X^2 + c_3 Y + c_2 X + c_1 \}$

タイプ52のイデアルのグレブナ基底 = $\{ X Y + a_4 X^2 + a_3 Y + a_2 X + a_1,$
 $Y^2 + b_4 X^2 + b_3 Y + b_2 X + b_1 \}$

タイプ53のイデアルのグレブナ基底 = $\{ X Y + a_4 X^2 + a_3 Y + a_2 X + a_1,$
 $X^3 + b_5 Y^2 + b_4 X^2 + b_3 Y + b_2 X + b_1 \}$

タイプ54のイデアルのグレブナ基底 = $\{ X^2 + a_3 Y + a_2 X + a_1,$
 $X Y^2 + b_5 Y^2 + b_4 X Y + b_3 Y + b_2 X + b_1 \}$

【 0 0 2 6 】

(位数4のイデアル)

位数4のイデアルIも同様にして、以下のようにタイプ41からタイプ44に分類される。

タイプ41のイデアルのグレブナ基底 = $\{ X Y + a_4 X^2 + a_3 Y + a_2 X + a_1,$
 $Y^2 + b_4 X^2 + b_3 Y + b_2 X + b_1,$

$X^3 + c_4 X^2 + c_3 Y + c_2 X + c_1 \}$

タイプ42のイデアルのグレブナ基底 = $\{ X^2 + a_3 Y + a_2 X + a_1,$
 $X Y + b_3 Y + b_2 X + b_1 \}$

タイプ43のイデアルのグレブナ基底 = $\{X^2 + a_3 Y + a_2 X + a_1, Y^2 + b_4 X Y + b_3 Y + b_2 X + b_1\}$

タイプ44のイデアルのグレブナ基底 = $\{Y + a_2 X + a_1\}$

【 0 0 2 7 】

(位数3のイデアル)

位数3のイデアルIも同様にして、以下のようにタイプ31からタイプ33に分類される。

タイプ31のイデアルのグレブナ基底 = $\{X^2 + a_3 Y + a_2 X + a_1, X Y + b_3 Y + b_2 X + b_1, Y^2 + c_3 Y + c_2 X + c_1\}$

タイプ32のイデアルのグレブナ基底 = $\{Y + a_2 X + a_1, X^3 + b_3 X^2 + b_2 X + b_1\}$

タイプ33のイデアルのグレブナ基底 = $\{X + a_1\}$

【 0 0 2 8 】

(位数2のイデアル)

位数2のイデアルIも同様にして、以下のようにタイプ21とタイプ22に分類される。

タイプ21のイデアルのグレブナ基底 = $\{Y + a_2 X + a_1, X^2 + b_2 X + b_1\}$

タイプ22のイデアルのグレブナ基底 = $\{X + a_1, Y^2 + b_2 Y + b_1\}$

【 0 0 2 9 】

(位数1のイデアル)

位数1のイデアルはもちろん以下のタイプ11のみである。

タイプ11のイデアルのグレブナ基底 = $\{X + a_1, Y + b_1\}$

【 0 0 3 0 】

[注意]

以上のイデアルタイプのうち、タイプ65, 44, 33は主イデアルであり、ヤコビ群要素として単位元を表す。また、以上のイデアルタイプのうち、reduced なイデアルタイプは31, 21, 22, 11のみである。例えば、タイプ32のイデアルがreducedでないのは以下のようにしてわかる。

【0 0 3 1】

I をタイプ32のイデアルとすると、 $f_I = Y + a_2 X + a_1$

よって、 $\text{ord}(I^*) = -v_\infty(f_I) - \delta(I) = 4 - 3 = 1$.

よって、 I^* はタイプ11なので、 $f_{I^*} = X + a'$ であり、

$\text{ord}(I^{**}) = -v_\infty(f_{I^*}) - \delta(I^*) = 3 - 1 = 2$.

位数が異なることから、 $I \neq I^{**}$.

【0 0 3 2】

[C₃₄曲線のヤコビ群加算アルゴリズム その2]

定義式 F をもつ体 k 上定義されたC₃₄曲線 C の座標環を $R=k[X, Y]/F$ とおく。ヤコビ群加算アルゴリズム 1 をより具体化し、その実行速度を見積もる。ただし、以下では、離散対数型暗号への応用を念頭にして、体 k の位数は十分に大きいとする。

【0 0 3 3】

(合成操作1)

まず、異なるイデアル I_1, I_2 に対して、ヤコビ群加算アルゴリズム 1 の第1ステップ、以下合成操作1と呼ぶ、を考察する。すなわち、イデアル積 $J=I_1 \cdot I_2$ に対して f_J を求める。そのためには、イデアル積 J のグレブナ基底を求めればよい(f_J はその第一要素)。C₃₄曲線の種数は3なので、加算対象となるイデアルの位数は3以下である。よって、そのタイプは11, 21, 22, 31, 32のいずれかである。ここでは、イデアル I_1, I_2 がともにタイプ31の場合を述べるが、他の場合も同様である。

【0 0 3 4】

I_1, I_2 を共にタイプ31の異なるイデアルとする。 I_1, I_2 がヤコビ群からランダムに選ばれたとすると、体 k の位数は十分に大きいとしているので、イデアル I に対してその解集合を $V(I)$ とかくとき、ほとんどの場合、

$$V(I_1) \cap V(I_2) = \phi \quad (1)$$

である (ϕ は空集合を表す)。条件(1)を満たさない場合も、 $R_1 + R_2 = 0$ となる要素 R_i を生成し、 $I_1 + I_2$ の代わりに $(I_1+R_1)+(I_2+R_2)$ を計算すれば、条件(1)が成り立つ場合に帰着する。また、条件(1)を満たさない場合は、非常に稀である(定義体 k のサイズを q とするととき $1/q$ 程度)ので、アルゴリズムの効率を評価する際には、条件(1)を満たしている場合のみ考察すればよい。そこで、以下では I

I_1, I_2 に対して条件(1)を仮定する。

【 0 0 3 5 】

$J=I_1 I_2$ を I_1 と I_2 の R におけるイデアル積とする。 I_1, I_2 は共に位数3なので J の位数は6となる。よって、 J のタイプは61, 62, 63, 64もしくは65である。 J のタイプがそのいずれであるかを定めるには、10個の単項式

$$1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, X^4 \quad (2)$$

の間の剰余環 R/J における線形関係を求めればよい。

【 0 0 3 6 】

イデアル I_i ($i=1, 2$)はタイプ31なので、

【数 1】

$$\begin{aligned} R/I_i &\cong k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \\ m &\mapsto v_m^{(i)} \end{aligned}$$

である。条件(1)より、

【数 2】

$$\begin{aligned} R/J &\cong R/I_1 \oplus R/I_2 \cong \bigoplus_{i=1}^6 k \\ m &\mapsto (m \bmod(I_1), m \bmod(I_2)) \mapsto v_m^{(1)} : v_m^{(2)} \end{aligned}$$

となる。

【 0 0 3 7 】

ここで、 $v^{(1)}_m : v^{(2)}_m$ は2つのベクトル $v^{(i)}_m$ ($i=1, 2$)を連結して得られる k 上の6次元ベクトルである。よって、式(2)中の10個の単項式 m_i 間の R/J での線形関係を求めるためには、ベクトル $v^{(1)}_{m_i} : v^{(2)}_{m_i}$ ($i=1, 2, \dots, 10$)を行とする、以下の10 x 6行列 M_C の行間の線形関係を求めればよい。

【数 3】

$$M_C = \begin{pmatrix} v_1^{(1)} : v_1^{(2)} \\ v_x^{(1)} : v_x^{(2)} \\ v_y^{(1)} : v_y^{(2)} \\ v_{x^2}^{(1)} : v_{x^2}^{(2)} \\ v_{xy}^{(1)} : v_{xy}^{(2)} \\ v_{y^2}^{(1)} : v_{y^2}^{(2)} \\ v_{x^3}^{(1)} : v_{x^3}^{(2)} \\ v_{x^2y}^{(1)} : v_{x^2y}^{(2)} \\ v_{xy^2}^{(1)} : v_{xy^2}^{(2)} \\ v_{x^4}^{(1)} : v_{x^4}^{(2)} \end{pmatrix}$$

行列 M_C の行間の線形関係は、よく知られているように、行縮約変換によって行列 M_C を三角化することにより得られ、これよりイデアル J のタイプとそのグレブナ基底を得る。詳細は実施例で述べる。

【 0 0 3 8】

(注意)

イデアル I_1, I_2 に対し、条件(1)が成立しない場合は、行列 M_C のランクが5以下となる。 I_1, I_2 のイデアル積を計算する際、最初はこれらに対して条件(1)を仮定して計算し、行縮約変換の結果、行列 M_C のランクが5以下であることが判明すれば、 $R_1 + R_2 = 0$ となる要素 R_i を生成し、 $I_1 + I_2$ の代わりに $(I_1+R_1)+(I_2+R_2)$ を計算すればよい。

【 0 0 3 9】

(合成操作2)

座標環 $R=k[X, Y]/F$ の同じイデアル $I_1=I, I_2=I$ に対する、ヤコビ群加算アルゴリズム 1 の第一ステップ、以下合成操作2と呼ぶ、を考察する。すなわち、イデアル積 $J=I^2$ に対して、そのグレブナ基底を求め、 f_J を計算する。イデアル I がタイプ3 1の場合を述べるが、他の場合も同様である。体 k の位数は十分に大きいとしているので、ほとんどの場合、 $V(I)$ には多重点はない。(3)

【 0 0 4 0】

また、アルゴリズムの効率を評価する際には、条件(3)を満たしている場合のみ

考察すればよい。以下ではIに対して条件(3)を仮定する。 $J=I^2$ はやはり位数6なので、そのグレブナ基底を計算するには、式(1)の単項式間の剰余環 R/J における船型関係を求めればよい。イデアルIはタイプ31なので、

【数 4】

$$\begin{aligned} R/I &\cong k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \\ m &\mapsto v_m \end{aligned}$$

である。また、条件(3)より、多項式 $f(\in R)$ が $J=I^2$ に属するための必要十分条件は、

$$f \in I, f_X F_Y - f_Y F_X \in I$$

である(ここで、多項式 f に対してその X による微分を f_X と書く。 f_Y に関しても同様。)。よって、

【数 5】

$$\begin{aligned} R/J &\cong R/I \oplus R/I \cong \bigoplus_{i=1}^6 k \\ m &\mapsto (m \bmod(I), m_X F_Y - m_Y F_X \bmod(I)) \mapsto v_m : v_{(m_X F_Y - m_Y F_X)} \end{aligned}$$

である。ここで、 $v_m : v_{(m_X F_Y - m_Y F_X)}$ は2つのベクトル $v_m, v_{(m_X F_Y - m_Y F_X)}$ を連結して得られる k 上の6次元ベクトルである。

結局、上記線形関係を求めるためには、式(1)中の10個の単項式 m_i に対して、 k 上の6次元ベクトル $v_{m_i} : v_{(m_i X F_Y - m_i Y F_X)}$ を行とする、以下の10 x 6行列 M_D の行間の線形関係を求めればよい。

【 0 0 4 1】

【数 6】

$$M_c = \begin{pmatrix} v_1 : 0 \\ v_x : v_{(F_Y)} \\ v_y : v_{(-F_X)} \\ v_{x^2} : v_{(2F_Y X)} \\ v_{xy} : v_{(-F_X X + F_Y Y)} \\ v_{y^2} : v_{(-2F_X Y)} \\ v_{x^3} : v_{(3F_Y X^2)} \\ v_{x^2 y} : v_{(-F_X X^2 + 2F_Y XY)} \\ v_{xy^2} : v_{(-2F_X XY + F_Y Y^2)} \\ v_{x^4} : v_{(4F_Y X^3)} \end{pmatrix}$$

以降は、合成操作1と同様に、行縮約変換によって行列 M_D を三角化すれば、イデアル J のタイプとそのグレブナ基底が得られる。

【 0 0 4 2】

(注意)

イデアル I に対し、条件(3)が成立しない場合は、行列 M_D のランクが5以下となる。 I^2 のグレブナ基底を計算する際、最初は条件(3)を仮定して計算し、行縮約変換の結果、行列 M_D のランクが5以下であることが判明すれば、 $R_1 + R_2 = 0$ となる要素 R_i を生成し、 $I + I$ の代わりに $(I+R_1)+(I+R_2)$ を計算すればよい。

【 0 0 4 3】

(還元操作)

ヤコビ群加算アルゴリズム 1 の第2ステップ(および第3ステップ)、以下還元操作と呼ぶ、を考察する。すなわち、位数6以下のイデアル J に対して、 $J^* = f_J : J$ のグレブナ基底を求める。以下、 J がタイプ61の場合を述べるが、その他の場合も同様である。

【 0 0 4 4】

J はタイプ61なのでそのグレブナ基底は、

$$\{f_J = X^3 + a_6 Y^2 + \dots, g = X^2 Y + b_6 Y^2 + \dots, h = X Y^2 + c_6 Y^2 + \dots\}$$

とかける。定義より $J^* = f_J : J$ なので、 $\delta(J^*) = -v_\infty(f_J) - \delta(J) = 3$ であ

る。よって、 J^* はreducedなので、 J^* はタイプ3Iのイデアルとなることがわかる。
よって、そのグレブナ基底を求めるには、

$$1, X, Y, X^2, XY, Y^2 \quad (4)$$

中の単項式 m_i に対して、 $\sum_i d_i m_i g$ と $\sum_i d_i m_i h$ が R/f_J で同時に0となる線形関係 $\sum_i d_i m_i$ を求めればよい。

$$LM(F)=Y^3, \quad LM(f_J) = X^3 \text{より、}$$

【数 7】

$$\begin{array}{ccc} R/f_J R \cong k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \oplus k \cdot X^2 \oplus k \cdot XY \oplus k \cdot Y^2 \oplus k \cdot X^2 Y \oplus k \cdot XY^2 \oplus k \cdot X^2 Y^2 \\ f \quad \mapsto \quad w_j \end{array}$$

なので、上記線形関係を求めるためには、式(4)の6個の各単項式 m_i に対して、2つのベクトル $w(m_i g)$, $w(m_i h)$ を連結して得られる k 上の18次元ベクトル $w(m_i g)$: $w(m_i h)$ を行とする、以下の6 x 18行列 M_R の行間の線形関係を求めればよい。

【 0 0 4 5】

【数 8】

$$M_R = \begin{pmatrix} w_g : w_h \\ w_{Xg} : w_{Xh} \\ w_{Yg} : w_{Yh} \\ w_{X^2g} : w_{X^2h} \\ w_{XYg} : w_{XYh} \\ w_{Y^2g} : w_{Y^2h} \end{pmatrix}$$

以降は、行縮約変換によって行列 M_R を三角化すれば、イデアル J^* のグレブナ基底が得られる。ただし、実はほとんどの場合、行列 M_R そのものではなく、その6 x 3のある部分行列 M_F を三角化すれば十分である。これについての詳細は次節で述べる。

【 0 0 4 6】

(アルゴリズムの演算量)

アルゴリズムの演算量を評価する。定義体の位数を q とおくとき、ヤコビ群のラ

ンダムな要素は、確率 $1/q$ の例外を除いて、タイプ31のイデアルで表される。また、タイプ31のイデアルに対する合成操作1, 2の結果は、確率 $1/q$ の例外を除いて、タイプ61のイデアルとなる。よって、アルゴリズムの演算量を評価するには、タイプ31のイデアルを入力したときの合成操作1, 2の演算量とタイプ61または31のイデアルを入力したときの還元操作の演算量を評価すればよい。また、以下では、アルゴリズムの演算量は乗算と逆数演算の回数で表す。

まず、合成操作1の演算量をみる。 I_1, I_2 をタイプ31のイデアルとする:

$$I_1 = \{X^2 + a_3 Y + a_2 X + a_1, X Y + b_3 Y + b_2 X + b_1, Y^2 + c_3 Y + c_2 X + c_1\}$$

$$I_2 = \{X^2 + s_3 Y + s_2 X + s_1, X Y + t_3 Y + t_2 X + t_1, Y^2 + u_3 Y + u_2 X + u_1\}$$

イデアル I_1, I_2 に対して、行列 M_C は

【数 9】

$$M_c = \begin{pmatrix} 1 & 0 & 0 & -a_1 & -b_1 & -c_1 & a_1 a_2 + a_3 b_1 & a_2 b_1 + a_3 c_1 & b_1 b_2 + b_3 c_1 & e_{10,1} \\ 0 & 1 & 0 & -a_2 & -b_2 & -c_2 & -a_1 + a_2^2 + a_3 b_2 & a_2 b_2 + a_3 c_2 & b_2^2 + b_3 c_2 & e_{10,2} \\ 0 & 0 & 1 & -a_3 & -b_3 & -c_3 & a_2 a_3 + a_3 b_3 & -a_1 + a_2 b_3 + a_3 c_3 & -b_1 + b_2 b_3 + b_3 c_3 & e_{10,3} \\ 1 & 0 & 0 & -s_1 & -t_1 & -u_1 & s_1 s_2 + s_3 t_1 & s_2 t_1 + s_3 u_1 & t_1 t_2 + t_3 u_1 & e_{10,4} \\ 0 & 1 & 0 & -s_2 & -t_2 & -u_2 & -s_1 + s_2^2 + s_3 t_2 & s_2 t_2 + s_3 u_2 & t_2^2 + t_3 u_2 & e_{10,5} \\ 0 & 0 & 1 & -s_3 & -t_3 & -u_3 & s_2 s_3 + s_3 t_3 & -s_1 + s_2 t_3 + s_3 u_3 & -t_1 + t_2 t_3 + t_3 u_3 & e_{10,6} \end{pmatrix}$$

と表示される。

【 0 0 4 7 】

ここで、

$$\begin{aligned} e_{10,1} &= a_1^2 - a_1 a_2^2 - 2a_2 a_3 b_1 - a_3^2 c_1 \\ e_{10,2} &= 2a_1 a_2 - a_2^3 - 2a_2 a_3 b_2 - a_3^2 c_2 \\ e_{10,3} &= 2a_1 a_3 - a_2^2 a_3 - 2a_2 a_3 b_3 - a_3^2 c_3 \\ e_{10,4} &= s_1^2 - s_1 s_2^2 - 2s_2 s_3 t_1 - s_3^2 u_1 \end{aligned}$$

$$e_{10,5} = 2s_1s_2 - s_2^3 - 2s_2s_3t_2 - s_3^2u_2$$

$$e_{10,6} = 2s_1s_3 - s_2^2s_3 - 2s_2s_3t_3 - s_3^2u_3$$

これより、重複をうまく取り除けば、行列 M_C は高々44回の乗算で構成できることがわかる。

【 0 0 4 8 】

行列 M_C' に対する行縮約変換は、その1行目から3行目までがすでに行縮約された形であり、成分が0または1であることに注意すると、3回の割算と高々 $6 \times 6 + 6 \times 5 + 6 \times 4 = 90$ 回の乗算で実行できる。以上より、合成操作1の演算量は高々逆数演算3、乗算134である。同様にして、合成操作2の演算量は高々逆数演算3、乗算214であることがわかる。行列 M_D が行列 M_C より複雑な分、演算量が増えている。

【 0 0 4 9 】

次に、タイプ61のイデアルを入力したときの縮約操作の演算量をみる。Jをタイプ61のイデアルとする：

$$J = \{ X^3 + a_6 Y^2 + a_5 X Y + a_4 X^2 + a_3 Y + a_2 X + a_1,$$

$$X^2 Y + b_6 Y^2 + b_5 X Y + b_4 X^2 + b_3 Y + b_2 X + b_1,$$

$$X Y^2 + c_6 Y^2 + c_5 X Y + c_4 X^2 + c_3 Y + c_2 X + c_1 \}$$

イデアルJに対する行列 M_R の第7列から第9列を取り出した 6×3 の小行列 M_r は

【数 1 0】

$$M_r = \begin{pmatrix} 1 & 0 & 0 \\ -a_4 - a_5 a_6 + b_5 & -a_5 - a_6^2 + b_6 & 0 \\ b_4 + a_5 b_6 & b_5 + a_6 b_6 & 1 \\ e_{4,1} & e_{4,2} & -a_5 - a_6^2 + b_6 \\ e_{5,1} & e_{5,2} & -a_4 - 2a_5 a_6 - a_6^3 + b_5 + a_6 b_6 \\ e_{6,1} & e_{6,2} & e_{6,3} \end{pmatrix}$$

となる。

【0 0 5 0】

ここで、

$$e_{4,1} = -a_2 + a_4^2 - a_3 a_6 + 3 a_4 a_5 a_6 + a_5^2 a_6^2 + b_3 - a_5 b_4 - a_4 b_5 - a_5 a_6 b_5$$

$$e_{4,2} = -a_3 + a_4 a_5 + a_5^2 a_6 + 2 a_4 a_6^2 + a_5 a_6^3 - a_6 b_4 - a_5 b_5 - a_6^2 b_5$$

$$e_{5,1} = -2 a_3 a_5 + 2 a_4 a_5^2 - a_2 a_6 + a_4^2 a_6 + a_5^3 a_6 - a_3 a_6^2 + 3 a_4 a_5 a_6^2 + a_5^2 a_6^3 + b_2 - a_4 b_4 - a_5 a_6 b_4 + a_3 b_6 - 2 a_4 a_5 b_6 - a_5^2 a_6 b_6$$

$$e_{5,2} = -a_2 + a_5^3 - 2 a_3 a_6 + 2 a_4 a_5 a_6 + 2 a_5^2 a_6^2 + 2 a_4 a_6^3 + a_5 a_6^4 + b_3 - a_5 b_4 - a_6^2 b_4 - a_5^2 b_6 - a_4 a_6 b_6 - a_5 a_6^2 b_6$$

$$e_{6,1} = -2 a_3 a_4 - 2 a_2 a_5 + 3 a_4^2 a_5 - 4 a_3 a_5 a_6 + 6 a_4 a_5^2 a_6 - a_2 a_6^2 + a_4^2 a_6^2 + 2 a_5^3 a_6^2 - a_3 a_6^3 + 3 a_4 a_5 a_6^3 + a_5^2 a_6^4 + a_5 b_3 + a_3 b_5 - 2 a_4 a_5 b_5 - a_5^2 a_6 b_5 + a_2 b_6 - a_4^2 b_6 + a_3 a_6 b_6 - 3 a_4 a_5 a_6 b_6 - a_5^2 a_6^2 b_6$$

$$e_{6,2} = -2 a_3 a_5 + 2 a_4 a_5^2 - 2 a_2 a_6 + a_4^2 a_6 + 2 a_5^3 a_6 - 3 a_3 a_6^2 + 5 a_4 a_5 a_6^2 + 3 a_5^2 a_6^3 + 2 a_4 a_6^4 + a_5 a_6^5 + b_2 + a_6 b_3 - a_5^2 b_5 - a_4 a_6 b_5 - a_5 a_6^2 b_5 + a_3 b_6 - a_4 a_5 b_6 - a_5^2 a_6 b_6 - 2 a_4 a_6^2 b_6 - a_5 a_6^3 b_6$$

$$e_{6,3} = -a_5^2 - 2 a_4 a_6 - 3 a_5 a_6^2 - a_6^4 + b_4 + a_6 b_5 + a_5 b_6 + a_6^2 b_6$$

である。

【0 0 5 1】

これより、行列 M_R の(2,2)成分 $d = -a_5 - a_6^2 + b_6$ が0でなければ、行列 M_R は階数3となる。よって、 $d \neq 0$ のとき、6 x 18行列 M_R の代わりに、その小行列である6 x 3行列の M_R を用いてよい。 $d = 0$ となる確率は $1/q$ 程度と考えられるので、アルゴリズムの効率を評価するさいには $d \neq 0$ としてよい。上式より、重複をうまく取り除けば、行列 M_R は高々40回の乗算で構成できることがわかる。行列 M_R' に対する行縮約変換は行列 M_R がすでに三角行列であり、その(1,1)および(3,3)成分が1であることに注意すると、高々1回の逆数演算と $2 \times 4 + 2 \times 3 = 14$ 回の乗算で実行できることがわかる。以上より、タイプ61のイデアルを入力としたとき、縮約操作の演算量は高々逆数演算1、乗算54である。タイプ31のイデアルを入力としたときも、同様な考察より、縮約操作は高々逆数演算1、乗算16であることが

わかる。

【 0 0 5 2 】

以上まとめると、本発明のヤコビ群加算アルゴリズムの演算量は図16 のようになる。図16中I, Mはそれぞれ逆数演算、乗算を表す。楕円曲線上では、(異なる要素の)加算は逆数演算1, 乗算3で、2倍算は逆数演算1, 乗算4で実行できる。ただし、同じビット長の群を得るには、有限体のビット長は C_{34} 曲線の場合の3倍となる。逆数演算の演算量を乗算のその20倍とし、逆数演算や乗算の演算量がビット長の2乗のオーダーであるとする、 C_{34} 曲線上の加算は楕円曲線上のその304/(23 x 9) \div 1.47倍、2倍算は384/(24 x 9) \div 1.78倍で実行できることがわかる。

【 0 0 5 3 】

【発明の実施の形態】

以下に、図面を用いて本発明の実施の形態につき詳細に説明する。図1は本発明の実施の形態の機能ブロック図であり、図2は図1のイデアル合成部の例を示すブロック図である。図3は図1の第一及び第二のイデアル縮約部の例を示すブロック図である。

【 0 0 5 4 】

まず、 C_{34} 曲線を用いた場合の実施例を示す。本実施例では、代数曲線パラメータファイルとして図4の代数曲線パラメータファイルを、イデアル型テーブルとして図5のイデアル型テーブルを、単項式リストテーブルとして図6の単項式リストテーブルを、グレブナ基底構成用テーブルとして図7のグレブナ基底構成用テーブルを用いる。

【 0 0 5 5 】

図1のヤコビ群要素加算装置において、図4の代数曲線パラメータファイルA16および代数曲線パラメータファイルA で指定された C_{34} 曲線のヤコビ群の要素を表す、代数曲線パラメータファイルAで指定された代数曲線の座標環のイデアルのグレブナ基底

$$I_1 = \{X^2 + 726 Y + 836 X + 355, X Y + 36 Y + 428 X + 477, Y^2 + 746 Y + 425 X + 865\}$$

および

$$I_2 = \{X^2 + 838 Y + 784 X + 97, X Y + 602 Y + 450 X + 291, Y^2 + 506 Y + 524 X + 497\}$$

が入力されたとする。

【 0 0 5 6 】

まず、イデアル合成部11が、図2に示す機能ブロックの処理の流れにしたがって、上記代数曲線パラメータファイルA、上記グレブナ基底 I_1 および I_2 を入力として以下のように動作する。まず、イデアル合成装置11は、図2のイデアル型分類部21において、図5のイデアル型テーブル25を参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル I_1 の型と一致するレコードを検索し第14レコードを得て、第14レコードのイデアル型番号フィールドの値 $N_1=31$ および位数フィールドの値 $d_1=3$ を取得する。

【 0 0 5 7 】

同様に、イデアル型が入力イデアル I_2 の型と一致するレコードを検索し第14レコードを得て、第14レコードのイデアル型番号フィールドの値 $N_2=31$ および位数フィールドの値 $d_2=3$ を取得する。

【 0 0 5 8 】

次に、イデアル合成部11は、単項式ベクトル生成部22において、前記位数フィールドの値 $d_1=3$ および $d_2=3$ の和 $d_3=d_1+d_2=6$ を計算し、単項式リストテーブル26を参照し前記 $d_3=6$ を位数フィールドの値に持つレコードを検索し第1レコードを得て、第1レコードの単項式リストフィールドに記述されている単項式のリスト1, X , Y , X^2 , $X Y$, Y^2 , X^3 , $X^2 Y$, $X Y^2$, X^4 を取得する。

【 0 0 5 9 】

I_1 と I_2 は異なっているので、前記単項式のリスト1, X , Y , X^2 , $X Y$, Y^2 , X^3 , $X^2 Y$, $X Y^2$, X^4 中のそれぞれの M_i ($1 \leq i \leq 10$) に対して、 M_i を I_1 で割った剰余を計算し、多項式 $a^{(i)}_1 + a^{(i)}_2 X + a^{(i)}_3 Y$ を得て、その係数を、代数曲線パラメータファイルAの単項式順序1, X , Y , ... の順にならべて、ベクトル $(a^{(i)}_1, a^{(i)}_2, a^{(i)}_3)$ を生成する。さらに、 M_i を I_2 で割った剰余を計算し、多項式 $b^{(i)}_1 + b^{(i)}_2 X + b^{(i)}_3 Y$ を得て、その係数を、代数曲線パラメータファイルAの単項式順

序1; X, Y, . . . の順にならべて、ベクトル $(b^{(i)}_1, b^{(i)}_2, b^{(i)}_3)$ を生成し、上記2つのベクトルを連結してベクトル $v_i = (a^{(i)}_1, a^{(i)}_2, a^{(i)}_3, b^{(i)}_1, b^{(i)}_2, b^{(i)}_3)$ を生成する。

【 0 0 6 0 】

すなわち、 $M_1 = 1$ を I_1 でわると、

$$1 = 0 \cdot (X^2 + 726 Y + 836 X + 355) + 0 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + 1$$

となるので、剰余として 1 を得て、ベクトル $(1, 0, 0)$ を生成する。 $M_1 = 1$ を I_2 でわると、

$$1 = 0 \cdot (X^2 + 838 Y + 784 X + 97) + 0 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + 1$$

となるので、剰余として 1 を得て、ベクトル $(1, 0, 0)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_1 = (1, 0, 0, 1, 0, 0)$ を生成する。

【 0 0 6 1 】

次に、 $M_2 = X$ を I_1 でわると、

$$X = 0 \cdot (X^2 + 726 Y + 836 X + 355) + 0 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + X$$

となるので、剰余として X を得て、ベクトル $(0, 1, 0)$ を生成する。 $M_2 = X$ を I_2 でわると、

$$1 = 0 \cdot (X^2 + 838 Y + 784 X + 97) + 0 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + X$$

となるので、剰余として X を得て、ベクトル $(0, 1, 0)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_2 = (0, 1, 0, 0, 1, 0)$ を生成する。

【 0 0 6 2 】

次に、 $M_3 = Y$ を I_1 でわると、

$$Y = 0 \cdot (X^2 + 726 Y + 836 X + 355) + 0 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + Y$$

となるので、剰余として Y を得て、ベクトル $(0, 0, 1)$ を生成する。 $M_3 = Y$ を I_2 でわると、

$$Y = 0 \cdot (X^2 + 838 Y + 784 X + 97) + 0 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + Y$$

となるので、剰余として Y を得て、ベクトル $(0, 0, 1)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_3 = (0, 0, 1, 0, 0, 1)$ を生成する。

【 0 0 6 3 】

次に、 $M_4 = X^2$ を I_1 でわると、

$$X^2 = 1 \cdot (X^2 + 726 Y + 836 X + 355) + 0 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + 654 + 173 X + 283 Y$$

となるので、剰余として $654 + 173 X + 283 Y$ を得て、ベクトル $(654, 173, 283)$ を生成する。 $M_4 = X^2$ を I_2 でわると、

$$X^2 = 1 \cdot (X^2 + 838 Y + 784 X + 97) + 0 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + 912 + 225 X + 171 Y$$

となるので、剰余として $912 + 225 X + 171 Y$ を得て、ベクトル $(912, 225, 171)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_4 = (654, 173, 283, 912, 225, 171)$ を生成する。

【 0 0 6 4 】

次に、 $M_5 = X Y$ を I_1 でわると、

$$X Y = 0 \cdot (X^2 + 726 Y + 836 X + 355) + 1 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + 532 + 581 X + 973 Y$$

となるので、剰余として $532 + 581 X + 973 Y$ を得て、ベクトル $(532, 581, 973)$ を生成する。 $M_5 = X Y$ を I_2 でわると、

$$X Y = 0 \cdot (X^2 + 838 Y + 784 X + 97) + 1 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + 718 + 559 X + 407 Y$$

となるので、剰余として $718 + 559 X + 407 Y$ を得て、ベクトル $(718, 559, 407)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_5 = (532, 581, 973, 718, 559, 407)$ を生成する。

【 0 0 6 5 】

次に、 $M_6 = Y^2$ を I_1 でわると、

$$Y^2 = 0 \cdot (X^2 + 726 Y + 836 X + 355) + 0 \cdot (X Y + 36 Y + 428 X + 477) + 1$$

$$\cdot (Y^2 + 746 Y + 425 X + 865) + 144 + 584 X + 263 Y$$

となるので、剰余として $144 + 584 X + 263 Y$ を得て、ベクトル $(144, 584, 263)$ を生成する。 $M_6 = Y^2$ を I_2 でわると、

$$Y^2 = 0 \cdot (X^2 + 838 Y + 784 X + 97) + 0 \cdot (X Y + 602 Y + 450 X + 291) + 1 \cdot (Y^2 + 506 Y + 524 X + 497) + 512 + 485 X + 503 Y$$

となるので、剰余として $512 + 485 X + 503 Y$ を得て、ベクトル $(512, 485, 503)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_6 = (144, 584, 263, 512, 485, 503)$ を生成する。

【 0 0 6 6 】

次に、 $M_7 = X^3$ を I_1 でわると、

$$X^3 = (173 + X) \cdot (X^2 + 726 Y + 836 X + 355) + 283 \cdot (X Y + 36 Y + 428 X + 477) + 0 \cdot (Y^2 + 746 Y + 425 X + 865) + 349 + 269 X + 429 Y$$

となるので、剰余として $349 + 269 X + 429 Y$ を得て、ベクトル $(349, 269, 429)$ を生成する。 $M_7 = X^3$ を I_2 でわると、

$$X^3 = (225 + X) \cdot (X^2 + 838 Y + 784 X + 97) + 171 \cdot (X Y + 602 Y + 450 X + 291) + 0 \cdot (Y^2 + 506 Y + 524 X + 497) + 53 + 821 X + 109 Y$$

となるので、剰余として $53 + 821 X + 109 Y$ を得て、ベクトル $(53, 821, 109)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_7 = (349, 269, 429, 53, 821, 109)$ を生成する。

【 0 0 6 7 】

次に、 $M_8 = X^2 Y$ を I_1 でわると、

$$X^2 Y = Y \cdot (X^2 + 726 Y + 836 X + 355) + 173 \cdot (X Y + 36 Y + 428 X + 477) + 283 \cdot (Y^2 + 746 Y + 425 X + 865) + 609 + 418 X + 243 Y$$

となるので、剰余として $609 + 418 X + 243 Y$ を得て、ベクトル $(609, 418, 243)$ を生成する。 $M_8 = X^2 Y$ を I_2 でわると、

$$X^2 Y = Y \cdot (X^2 + 838 Y + 784 X + 97) + 225 \cdot (X Y + 602 Y + 450 X + 291) + 171 \cdot (Y^2 + 506 Y + 524 X + 497) + 888 + 856 X + 916 Y$$

となるので、剰余として $888 + 856 X + 916 Y$ を得て、ベクトル $(888, 856, 916)$ を生成する。これら2つのベクトルを連結して、ベクトル $v_8 = (609, 418, 243, 888, 856, 916)$ を生成する。

56,916)を生成する。

【 0 0 6 8 】

次に、 $M_9 = X Y^2$ を I_1 でわると、

$$X Y^2 = 0 \cdot (X^2 + 726 Y + 836 X + 355) + (581+Y) \cdot (X Y + 36 Y + 428 X + 477) + 973 \cdot (Y^2 + 746 Y + 425 X + 865) + 199 + 720 X + 418 Y$$

となるので、剰余として $199 + 720 X + 418 Y$ を得て、ベクトル(199,720,418)を生成する。 $M_9 = X Y^2$ を I_2 でわると、

$$X Y^2 = 0 \cdot (X^2 + 838 Y + 784 X + 97) + (559+Y) \cdot (X Y + 602 Y + 450 X + 291) + 407 \cdot (Y^2 + 506 Y + 524 X + 497) + 310 + 331 X + 91 Y$$

となるので、剰余として $310 + 331 X + 91 Y$ を得て、ベクトル(310,331,91)を生成する。これら2つのベクトルを連結して、ベクトル $v_9=(199,720,418,310,331,91)$ を生成する。

【 0 0 6 9 】

次に、 $M_{10} = X^4$ を I_1 でわると、

$$X^4 = (313 + 173 X + X^2 + 283 Y) \cdot (X^2 + 726 Y + 836 X + 355) + 45 \cdot (X Y + 36 Y + 428 X + 477) + 378 \cdot (Y^2 + 746 Y + 425 X + 865) + 554 + 498 X + 143 Y$$

となるので、剰余として $554 + 498 X + 143 Y$ を得て、ベクトル(554,498,143)を生成する。 $M_{10} = X^4$ を I_2 でわると、

$$X^4 = (78 + 225 X + X^2 + 171 Y) \cdot (X^2 + 838 Y + 784 X + 97) + 266 \cdot (X Y + 602 Y + 450 X + 291) + 989 \cdot (Y^2 + 506 Y + 524 X + 497) + 643 + 522 X + 107 Y$$

となるので、剰余として $643 + 522 X + 107 Y$ を得て、ベクトル(643,522,107)を生成する。これら2つのベクトルを連結して、ベクトル $v_{10}=(554,498,143,643,522,107)$ を生成する。以上で、イデアル合成部11の、単項式ベクトル生成部22における処理を終了する。

【 0 0 7 0 】

次に、イデアル合成部11は、基底構成部23において、単項式ベクトル生成部22で生成した、10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ を線形関係導

出部24に入力し、出力として複数の10次元ベクトル m_1, m_2, \dots を得る。線形関係導出部24は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術であるので、以下、線形関係導出部24の動作はその概略のみ示す。

【0 0 7 1】

線形関係導出部24は、まず、入力された10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ を順に並べて10x6行列

【数 1 1】

$$M_c = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 654 & 173 & 283 & 912 & 225 & 171 \\ 532 & 581 & 973 & 718 & 559 & 407 \\ 144 & 584 & 263 & 512 & 485 & 503 \\ 349 & 269 & 429 & 53 & 821 & 109 \\ 609 & 418 & 243 & 888 & 856 & 916 \\ 199 & 720 & 418 & 310 & 331 & 91 \\ 554 & 498 & 143 & 643 & 522 & 107 \end{pmatrix}$$

を構成する。

【0 0 7 2】

次に、線形関係導出部24は、行列 M_c に10次元の単位行列を連結し、

【数 1 2】

$$M_c = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 654 & 173 & 283 & 912 & 225 & 171 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 532 & 581 & 973 & 718 & 559 & 407 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 144 & 584 & 263 & 512 & 485 & 503 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 349 & 269 & 429 & 53 & 821 & 109 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 609 & 418 & 243 & 888 & 856 & 916 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 199 & 720 & 418 & 310 & 331 & 91 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 554 & 498 & 143 & 643 & 522 & 107 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

を得る。

【 0 0 7 3 】

次に、線形関係導出部24は、 i 行目の定数倍を $i+1$ 行目から10行目に加えることで ($i=1, 2, \dots, 6$)、行列 M'_C を三角化し以下の行列 m を得る。

【数 1 3】

$$m = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 258 & 52 & 897 & 355 & 836 & 726 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 621 & 688 & 268 & 365 & 592 & 187 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 31 & 514 & 469 & 637 & 669 & 155 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 28 & 132 & 31 & 271 & 469 & 166 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 856 & 618 & 747 & 909 & 132 & 636 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 652 & 322 & 240 & 978 & 826 & 846 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 333 & 346 & 980 & 935 & 824 & 614 & 0 & 0 & 0 & 1 \end{pmatrix}$$

【 0 0 7 4 】

よく知られているように行列 m の7から10行目の第7成分以降よりなるベクトルは、入力された10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ の全ての1次独立な線形従属関係 $\sum_{i=1}^{10} m_{ji} v_i = 0$ ($j=1, 2, \dots$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,n}), (m_{2,1}, m_{2,2}, \dots, m_{2,n}), \dots\}$ である。線形関係導出部24は、行列 m の7行目の第7成分以降よりなるベクトル $m_1=(28, 132, 31, 271, 469, 166, 1, 0, 0, 0)$ 、行列 m の8行目の第7成分以降よりなるベクトル $m_2=(856, 618, 747, 909, 132, 636, 0, 1, 0, 0)$ 、行列 m の9行目の第7成分以降よりなるベクトル $m_3=(652, 322, 240, 978, 826, 846, 0, 0, 1, 0)$ および行列 m の10行目の第7成分以降よりなるベクトル $m_4=(333, 346, 980, 935, 824, 614, 0, 0, 0, 1)$ を出力する。イデアル合成部11の基底構成部23における処理の説明に戻る。

【 0 0 7 5 】

次に、イデアル合成装置11は、図7のグレブナ基底構成用テーブル27を参照し前記値 $d_3=6$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(28, 132, 31, 271, 469, 166, 1, 0, 0, 0)$ 、 $m_2=(856, 618, 747, 909, 132, 636, 0, 1, 0, 0)$ 、 $m_3=(652, 322, 240, 978, 826, 846, 0, 0, 1, 0)$ 、

1, 0)および $m_4=(333, 346, 980, 935, 824, 614, 0, 0, 0, 1)$ 中に存在しないレコードを検索する。第1レコードの位数フィールドの値は6であり、第1レコードの成分番号リスト7, 8, 9, 10がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第1レコードが得られる。

【 0 0 7 6 】

さらに第1レコードの第一ベクトル型の値は(*, *, *, *, *, *, 1, 0, 0, 0)であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(28, 132, 31, 271, 469, 166, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 , $X^2 Y$, X Y^2 , X^4 の各単項式の係数の列とみなし、多項式 $f_1=28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ を生成する。

【 0 0 7 7 】

同様にして、第1レコードの第二ベクトル型の値は(*, *, *, *, *, *, 0, 1, 0, 0)であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(856, 618, 747, 909, 132, 636, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 , $X^2 Y$, X Y^2 , X^4 の各単項式の係数の列とみなし、

多項式 $f_2=856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y$ を生成する。

【 0 0 7 8 】

同様にして、第1レコードの第三ベクトル型の値は(*, *, *, *, *, *, 0, 0, 1, 0)であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_3=(652, 322, 240, 978, 826, 846, 0, 0, 1, 0)$ と合致するので、ベクトル m_3 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 , $X^2 Y$, X Y^2 , X^4 の各単項式の係数の列とみなし、多項式 $f_3=652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2$ を生成する。最後に、イデアル合成部11は、多項式の集合 $J=\{f_1, f_2, f_3\}$ を構成し、出力する。以上で、イデアル合成部11の動作は終了する。

【 0 0 7 9 】

次に、第一のイデアル縮約部12が、図3に示す機能ブロックの処理の流れにした

がって、図4の代数曲線パラメータファイルAおよびイデアル合成部11が出力したグレブナ基底

$$J = \{ 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3, \\ 856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y, \\ 652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2 \}$$

を入力として以下のように動作する。

【 0 0 8 0 】

まず、イデアル縮約部12は、図3のイデアル型分類部31において、図5のイデアル型テーブル35を参照し、イデアル型フィールドに記述されているイデアル型が入力イデアルJの型と一致するレコードを検索し第1レコードを得て、第1レコードのイデアル型番号フィールドの値N=61および縮約位数フィールドの値d=3を取得する。次に、イデアル縮約部12は、前記d=3が0でないことを確認し、多項式ベクトル生成部32において、単項式リストテーブル36を参照し前記d=3を位数フィールドの値に持つレコードを検索し第4レコードを得て、第4レコードの単項式リストフィールドに記述されている単項式のリスト1, X, Y, X², X Y, Y², X³を取得する。

【 0 0 8 1 】

さらに、イデアル縮約部12は、多項式ベクトル生成部32において、Jの第1要素f=28 + 132 X + 31 Y + 271 X² + 469 X Y + 166 Y² + X³、第2要素g=856 + 618 X + 747 Y + 909 X² + 132 X Y + 636 Y² + X² Yおよび第3要素h=652 + 322 X + 240 Y + 978 X² + 826 X Y + 846 Y² + X Y²を取得し、代数曲線パラメータファイルAの係数リスト0, 7, 0, 0, 0, 0, 0, 0, 1, 1を、代数曲線パラメータファイルAの単項式順序1, X, Y, X², X Y, Y², X³, X² Y, X Y², X⁴, Y³の各単項式の係数の列とみなして、定義多項式F=Y³+X⁴+7Xを生成する。

【 0 0 8 2 】

次に、イデアル縮約部12は、多項式ベクトル生成部32において、前記単項式のリスト1, X, Y, X², X Y, Y², X³中のそれぞれのM_i (1<=i<=7) に対して、M_iと多項式gの積M_i・gの、多項式fおよびFによる剰余式r_iを計算し、その係数を、代数曲線パラメータファイルAの単項式順序1, X, Y, . . . の順にならべて、ベクトルw

(i)₁を生成する。さらに、 M_i と多項式 h の積 $M_i \cdot h$ の、多項式 f および F による剰余式 s_i を計算し、その係数を、代数曲線パラメータファイルAの単項式順序1, X, Y, . . . の順にならべて、ベクトル $w^{(i)}_2$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル v_i を生成する。

【 0 0 8 3 】

すなわち、まず、第一番目の単項式 $M_1=1$ に対して、

$1 \cdot g = 856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y$ を
 $f=28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F=Y^3+X^4+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y$ となるので、剰余 $856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y$ を得て、ベクトル $w^{(1)}_1=(856, 618, 747, 909, 132, 636, 1, 0, 0)$ を生成する。

【 0 0 8 4 】

また、 $1 \cdot h=652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2$ を $f=28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F=Y^3+X^4+7X$ で割ると、 $h = 0 \cdot f + 0 \cdot F + 652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2$ となるので、剰余 $652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2$ を得て、ベクトル $w^{(1)}_2=(652, 322, 240, 978, 826, 846, 0, 1, 0)$ を生成する。そして、ベクトル $w^{(1)}_1$ と $w^{(1)}_2$ を連結して、ベクトル $v_1=(856, 618, 747, 909, 132, 636, 1, 0, 0, 652, 322, 240, 978, 826, 846, 0, 1, 0)$ を得る。

【 0 0 8 5 】

次に、第二番目の単項式 $M_2=X$ に対して、 $X g = X (856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f=28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F=Y^3+X^4+7X$ で割ると、 $X g = (319 + 166 X + Y) f + 843 F + 149 + 667 X + 220 X^2 + 173 Y + 235 X Y + 709 X^2 Y + 492 Y^2 + 863 X Y^2$ となるので、剰余 $149 + 667 X + 220 X^2 + 173 Y + 235 X Y + 709 X^2 Y + 492 Y^2 + 863 X Y^2$ を得て、ベクトル $w^{(2)}_1=(149, 667, 173, 220, 235, 492, 709, 863, 0)$ を生成する。

【 0 0 8 6 】

また、 $X h = X (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X h = 978 f + 0 \cdot F + 868 + 708 X + 651 X^2 + 961 Y + 653 X Y + 826 X^2 Y + 101 Y^2 + 846 X Y^2 + X^2 Y^2$ となるので、剰余 $868 + 708 X + 651 X^2 + 961 Y + 653 X Y + 826 X^2 Y + 101 Y^2 + 846 X Y^2 + X^2 Y^2$ を得て、ベクトル $w^{(2)}_2 = (868, 708, 961, 651, 653, 101, 826, 846, 1)$ を生成する。そして、ベクトル $w^{(2)}_1$ と $w^{(2)}_2$ を連結して、ベクトル $v_2 = (149, 667, 173, 220, 235, 492, 709, 863, 0, 868, 708, 961, 651, 653, 101, 826, 846, 1)$ を得る。

【 0 0 8 7 】

次に、第三番目の単項式 $M_3 = Y$ に対して、 $Y g = Y (856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $Y g = (826 + 373 X) f + 636 F + 79 + 179 X + 357 X^2 + 475 Y + 216 X Y + 529 X^2 Y + 855 Y^2 + 772 X Y^2 + X^2 Y^2$ となるので、剰余 $79 + 179 X + 357 X^2 + 475 Y + 216 X Y + 529 X^2 Y + 855 Y^2 + 772 X Y^2 + X^2 Y^2$ を得て、ベクトル $w^{(3)}_1 = (79, 179, 475, 357, 216, 855, 529, 772, 1)$ を生成する。

【 0 0 8 8 】

また、 $Y h = Y (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $Y h = (327 + 595 X + 1008 X^2 + 469 Y) f + (685 + X) F + 934 + 966 X + 358 X^2 + 590 Y + 694 X Y + 473 X^2 Y + 31 Y^2 + 939 X Y^2 + 166 X^2 Y^2$ となるので、剰余 $934 + 966 X + 358 X^2 + 590 Y + 694 X Y + 473 X^2 Y + 31 Y^2 + 939 X Y^2 + 166 X^2 Y^2$ を得てベクトル $w^{(3)}_2 = (934, 966, 590, 358, 694, 31, 473, 939, 166)$ を生成する。そして、ベクトル $w^{(3)}_1$ と $w^{(3)}_2$ を連結して、ベクトル $v_3 = (79, 179, 475, 357, 216, 855, 529, 772, 1, 934, 966, 590, 358, 694, 31, 473, 939, 166)$ を得る。

【 0 0 8 9 】

次に、第四番目の単項式 $M_4 = X^2$ に対して、 $X^2 g = X^2 (856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X^2 g = (645 + 969 X + 166 X^2 + 7$

$$09 \cdot Y' + X \cdot Y) f + (359 + 843 X) F + 102 + 241 X + 394 X^2 + 513 Y + 647 X Y \\ + 683 X^2 Y + 103 Y^2 + 1004 X Y^2 + 863 X^2 Y^2$$

となるので、剰余 $102 + 241 X + 394 X^2 + 513 Y + 647 X Y + 683 X^2 Y + 103 Y^2 + 1004 X Y^2 + 863 X^2 Y^2$ を得て、ベクトル $w^{(4)}_1 = (102, 241, 513, 394, 647, 103, 683, 1004, 863)$ を生成する。

【 0 0 9 0 】

また、 $X^2 h = X^2 (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X^2 h = (725 + 16 X + 782 X^2 + 754 Y + 166 X Y + Y^2) f + (930 + 227 X + 843 Y) F + 889 + 260 X + 560 X^2 + 809 Y + 425 X Y + 552 X^2 Y + 535 Y^2 + 671 X Y^2 + 763 X^2 Y^2$ となるので、剰余 $889 + 260 X + 560 X^2 + 809 Y + 425 X Y + 552 X^2 Y + 535 Y^2 + 671 X Y^2 + 763 X^2 Y^2$ を得て、ベクトル $w^{(4)}_2 = (889, 260, 809, 560, 425, 535, 552, 671, 763)$ を生成する。そして、ベクトル $w^{(4)}_1$ と $w^{(4)}_2$ を連結して、ベクトル $v_4 = (102, 241, 513, 394, 647, 103, 683, 1004, 863, 889, 260, 809, 560, 425, 535, 552, 671, 763)$ を得る。

【 0 0 9 1 】

次に、第五番目の単項式 $M_5 = X Y$ に対して、 $X Y g = X Y (856 + 618 X + 747 Y + 909 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X Y g = (95 + 3 X + 146 X^2 + 457 Y + 166 X Y + Y^2) f + (791 + 863 X + 843 Y) F + 367 + X + 54 X^2 + 403 Y + 361 X Y + 276 X^2 Y + 305 Y^2 + 600 X Y^2 + 689 X^2 Y^2$ となるので、剰余 $367 + X + 54 X^2 + 403 Y + 361 X Y + 276 X^2 Y + 305 Y^2 + 600 X Y^2 + 689 X^2 Y^2$ を得て、ベクトル $w^{(5)}_1 = (367, 1, 403, 54, 361, 305, 276, 600, 689)$ を生成する。

【 0 0 9 2 】

また、 $X Y h = X Y (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X Y h = (804 + 648 X + 246 X^2 + 1008 X^3 + 629 Y + 782 X Y + 166 Y^2) f + (421 + 25 X + X^2 + 696 Y) F + 695 + 924 X + 289 X^2 + 851 Y + 210 X Y + 321 X^2 Y + 802 Y^2 + 522 X Y^2 + 278 X^2 Y^2$ となるので、剰余 $695 + 924 X + 289 X^2 + 851 Y + 210 X Y + 321 X^2 Y + 802 Y^2 + 522 X Y^2 + 278 X^2 Y^2$ を得る。

$4 X + 289 X^2 + 851 Y + 210 X Y + 321 X^2 Y + 802 Y^2 + 522 X Y^2 + 278 X^2 Y$
 2 を得て、ベクトル $w^{(5)}_2 = (695, 924, 851, 289, 210, 802, 321, 522, 278)$ を生成する。
 そして、ベクトル $w^{(5)}_1$ と $w^{(5)}_2$ を連結して、ベクトル $v_5 = (367, 1, 403, 54, 361, 305$
 $, 276, 600, 689, 695, 924, 851, 289, 210, 802, 321, 522, 278)$ を得る。

【 0 0 9 3 】

次に、第六番目の単項式 $M_6 = Y^2$ に対して、 $Y^2 g = Y^2 (856 + 618 X + 747 Y + 9$
 $09 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y$
 $+ 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $Y^2 g = (687 + 214 X + 320 X^2 + 1$
 $008 X^3 + 77 Y + 146 X Y + 166 Y^2) f + (981 + 960 X + X^2 + 323 Y) F + 944$
 $+ 384 X + 956 X^2 + 763 Y + 737 X Y + 925 X^2 Y + 859 Y^2 + 416 X Y^2 + 814$
 $X^2 Y^2$ となるので、剰余 $944 + 384 X + 956 X^2 + 763 Y + 737 X Y + 925 X^2 Y +$
 $859 Y^2 + 416 X Y^2 + 814 X^2 Y^2$ を得て、ベクトル $w^{(6)}_1 = (944, 384, 763, 956,$
 $737, 859, 925, 416, 814)$ を生成する。

【 0 0 9 4 】

また、 $Y^2 h = Y^2 (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$
 を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で
 割ると、 $Y^2 h = (260 + 17 X + 731 X^2 + 843 X^3 + 382 Y + 246 X Y + 1008 X^2$
 $Y + 782 Y^2) f + (369 + 868 X + 166 X^2 + 186 Y + X Y) F + 792 + 963 X + 643$
 $X^2 + 415 Y + 539 X Y + 887 X^2 Y + 438 Y^2 + 102 X Y^2 + 363 X^2 Y^2$ となるの
 で、剰余 $792 + 963 X + 643 X^2 + 415 Y + 539 X Y + 887 X^2 Y + 438 Y^2 + 102$
 $X Y^2 + 363 X^2 Y^2$ を得て、ベクトル $w^{(6)}_2 = (792, 963, 415, 643, 539, 438, 88$
 $7, 102, 363)$ を生成する。そして、ベクトル $w^{(6)}_1$ と $w^{(6)}_2$ を連結して、ベクトル
 $v_6 = (944, 384, 763, 956, 737, 859, 925, 416, 814, 792, 963, 415, 643, 539,$
 $438, 887, 102, 363)$ を得る。

【 0 0 9 5 】

最後に、第七番目の単項式 $M_7 = X^3$ に対して、 $X^3 g = X^3 (856 + 618 X + 747 Y +$
 $909 X^2 + 132 X Y + 636 Y^2 + X^2 Y)$ を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X$
 $Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で割ると、 $X^3 g = (323 + 583 X + 814 X^2 +$
 $166 X^3 + 96 Y + 689 X Y + X^2 Y + 863 Y^2) f + (698 + 514 X + 843 X^2 + 20$

$Y) \cdot F + 37 + 730 X + 831 X^2 + 416 Y + 136 X Y + 55 X^2 Y + 971 Y^2 + 398 X$
 $Y^2 + 5 X^2 Y^2$ となるので、剰余 $37 + 730 X + 831 X^2 + 416 Y + 136 X Y + 55 X$
 $2 Y + 971 Y^2 + 398 X Y^2 + 5 X^2 Y^2$ を得て、ベクトル $w^{(7)}_1 = (37, 730, 416, 831, 1$
 $36, 971, 55, 398, 5)$ を生成する。

【 0 0 9 6 】

また、 $X^3 h = X^3 (652 + 322 X + 240 Y + 978 X^2 + 826 X Y + 846 Y^2 + X Y^2)$
 を $f = 28 + 132 X + 31 Y + 271 X^2 + 469 X Y + 166 Y^2 + X^3$ および $F = Y^3 + X^4 + 7X$ で
 割ると、 $X^3 h = (449 + 750 X + 363 X^2 + 782 X^3 + 102 Y + 278 X Y + 166 X^2$
 $Y + 763 Y^2 + X Y^2) f + (784 + 583 X + 227 X^2 + 476 Y + 843 X Y) F + 545 +$
 $9 X + 173 X^2 + 378 Y + 902 X Y + 16 X^2 Y + 831 Y^2 + 820 X Y^2 + 909 X^2 Y$
 2 となるので、剰余 $545 + 9 X + 173 X^2 + 378 Y + 902 X Y + 16 X^2 Y + 831 Y^2$
 $+ 820 X Y^2 + 909 X^2 Y^2$ を得て、ベクトル $w^{(7)}_2 = (545, 9, 378, 173, 902, 831, 16, 8$
 $20, 909)$ を生成する。そして、ベクトル $w^{(7)}_1$ と $w^{(7)}_2$ を連結して、ベクトル $v_7 = (3$
 $7, 730, 416, 831, 136, 971, 55, 398, 5, 545, 9, 378, 173, 902, 831, 16, 820, 909)$ を得る
 。以上で、第一のイデアル縮約部12の、多項式ベクトル生成部32における処理を
 終了する。

【 0 0 9 7 】

次に、第一のイデアル縮約部12は、基底構成部33において、多項式ベクトル生成
 部32で生成した、7個の18次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を線形関係導部34
 に入力し、出力として複数の7次元ベクトル m_1, m_2, \dots を得る。線形関係導出部34
 は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し
 法は既知の技術に属するので、以下、線形関係導出装置34の動作はその概略のみ
 示す。

【 0 0 9 8 】

線形関係導出部34は、まず、入力された7個の18次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6$
 $, v_7$ を順に並べて 7×18 行列

【数 1 4】

$$M_R =$$

856	618	747	909	132	636	1	0	0	652	322	240	978	826	846	0	1	0
149	667	173	220	235	492	709	863	0	868	708	961	651	653	101	826	846	1
79	179	475	357	216	855	529	772	1	934	966	590	358	694	31	473	939	166
102	241	513	394	647	103	683	1004	863	889	260	809	560	425	535	552	671	763
367	1	403	54	361	305	276	600	689	695	924	851	289	210	802	321	522	278
944	384	763	956	737	859	925	416	814	792	963	415	643	539	438	887	102	363
37	730	416	831	136	971	55	398	5	545	9	378	173	902	831	16	820	909

を構成する。

【0 0 9 9】

次に、線形関係導出装置34は、行列M_Rに7次元の単位行列を連結し、

【数 1 5】

$$M'_R = \begin{bmatrix} 856 & 618 & 747 & 909 & 132 & 636 & 1 & 0 & 0 & 652 & 322 & 240 & 978 & 826 & 846 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 149 & 667 & 173 & 220 & 235 & 492 & 709 & 863 & 0 & 868 & 708 & 961 & 651 & 653 & 101 & 826 & 846 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 79 & 179 & 475 & 357 & 216 & 855 & 529 & 772 & 1 & 934 & 966 & 590 & 358 & 694 & 31 & 473 & 939 & 166 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 102 & 241 & 513 & 394 & 647 & 103 & 683 & 1004 & 863 & 889 & 260 & 809 & 560 & 425 & 535 & 552 & 671 & 763 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 367 & 1 & 403 & 54 & 361 & 305 & 276 & 600 & 689 & 695 & 924 & 851 & 289 & 210 & 802 & 321 & 522 & 278 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 944 & 384 & 763 & 956 & 737 & 859 & 925 & 416 & 814 & 792 & 963 & 415 & 643 & 539 & 438 & 887 & 102 & 363 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 37 & 730 & 416 & 831 & 136 & 971 & 55 & 398 & 5 & 545 & 9 & 378 & 173 & 902 & 831 & 16 & 820 & 909 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

を構成する。

【 0 1 0 0 】

次に、線形関係導出装置34は、i行目の定数倍をi+1行目から7行目に加えること
で(i=1,2,3)、行列M' Rを三角化し以下の行列mを得る。

【 0 1 0 1 】

【数 1 6】

$$m = \begin{pmatrix} 856 & 618 & 747 & 909 & 132 & 636 & 1 & 0 & 0 & 652 & 322 & 240 & 978 & 826 & 846 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 62 & 485 & 393 & 47 & 320 & 677 & 863 & 0 & 184 & 494 & 344 & 634 & 455 & 272 & 826 & 814 & 1 & 977 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 252 & 630 & 861 & 845 & 645 & 389 & 1 & 380 & 422 & 1006 & 632 & 736 & 748 & 221 & 979 & 217 & 281 & 51 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 982 & 226 & 146 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 449 & 79 & 320 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 544 & 564 & 195 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 79 & 930 & 1004 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

よく知られているように行列 m の4から7行目の第19成分以降よりなるベクトルは、入力された7個の18次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ の全ての1次独立な線形従属関係 $\sum_{i=1}^7 m_{ji} v_i = 0$ ($j=1, 2, \dots, 7$)を表すベクトル $\{(m_1, 1, m_1, 2, \dots, m_1, 7), (m_2, 1, m_2, 2, \dots, m_2, 7), \dots\}$ である。線形関係導出部34は、行列 m の4行目の第19成分以降よりなるベクトル $m_1=(982, 226, 146, 1, 0, 0, 0)$ 、行列 m の5行目の第19成分以降よりなるベクトル $m_2=(449, 79, 320, 0, 1, 0, 0)$ 、行列 m の6行目の

第19成分以降よりなるベクトル $m_3=(544, 564, 195, 0, 0, 1, 0)$ および行列 m の7行目の第19成分以降よりなるベクトル $m_4=(79, 930, 1004, 0, 0, 0, 1)$ を出力する。

【0 1 0 2】

第一のイデアル縮約部12の基底構成部33における処理の説明に戻る。次に、このイデアル縮約部12は、図7のグレブナ基底構成用テーブル37を参照し前記値 $d=3$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(982, 226, 146, 1, 0, 0, 0)$ 、 $m_2=(449, 79, 320, 0, 1, 0, 0)$ 、 $m_3=(544, 564, 195, 0, 0, 1, 0)$ および $m_4=(79, 930, 1004, 0, 0, 0, 1)$ 中に存在しないレコードを検索する。第14レコードの位数フィールドの値は3であり、第14レコードの成分番号リスト4,5,6,7に対応する成分がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第14レコードが得られる。

【0 1 0 3】

さらに、第14レコードの第一ベクトル型の値は $(*, *, *, 1, 0, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(982, 226, 146, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_1=982 + 226 X + 146 Y + X^2$ を生成する。

【0 1 0 4】

同様にして、第14レコードの第二ベクトル型の値は $(*, *, *, 0, 1, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(449, 79, 320, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_2=449 + 79 X + 320 Y + X Y$ を生成する。

【0 1 0 5】

同様にして、第14レコードの第三ベクトル型の値は $(*, *, *, 0, 0, 1, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_3=(544, 564, 195, 0, 0, 1, 0)$ と合致するので、ベクトル m_3 を、代数曲線パラメータファイルAの単項式順

序1, X , Y , X^2 , $X Y$, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_3=544 + 564 X + 195 Y + Y^2$ を生成する。

【 0 1 0 6 】

最後に、イデアル縮約部12は、多項式の集合

$$J^* = \{f_1=982 + 226 X + 146 Y + X^2, f_2=449 + 79 X + 320 Y + X Y, f_3=544 + 564 X + 195 Y + Y^2\}$$

を構成し、出力する。以上で、第一のイデアル縮約部12の動作は終了する。

【 0 1 0 7 】

次に、第二のイデアル縮約部13が、図3に示す機能ブロック処理の流れに従って、図4の代数曲線パラメータファイルA30および第一のイデアル縮約部12が出力したグレブナ基底

$$J^* = \{982 + 226 X + 146 Y + X^2, 449 + 79 X + 320 Y + X Y, 544 + 564 X + 195 Y + Y^2\}$$

を入力として以下のように動作する。まず、第二のイデアル縮約部13は、図3のイデアル型分類部31において、図5のイデアル型テーブル35を参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル J^* の型と一致するレコードを検索し第14レコードを得て、第14レコードのイデアル型番号フィールドの値 $N=31$ および縮約位数フィールドの値 $d=3$ を取得する。

【 0 1 0 8 】

次に、イデアル縮約部13は、前記 $d=3$ が0でないことを確認し、多項式ベクトル生成部32において、単項式リストテーブル36を参照し前記 $d=3$ を位数フィールドの値に持つレコードを検索し第4レコードを得て、第4レコードの単項式リストフィールドに記述されている単項式のリスト1, X , Y , X^2 , $X Y$, Y^2 , X^3 を取得する。さらに、イデアル縮約部13は、 J^* の第1要素 $f=982 + 226 X + 146 Y + X^2$ 、第2要素 $g=449 + 79 X + 320 Y + X Y$ および第3要素 $h=544 + 564 X + 195 Y + Y^2$ を取得し、代数曲線パラメータファイルAの係数リスト0, 7, 0, 0, 0, 0, 0, 0, 0, 1, 1を、代数曲線パラメータファイルAの単項式順序1, X , Y , X^2 , $X Y$, Y^2 , X^3 , $X^2 Y$, $X Y^2$, X^4 , Y^3 の各単項式の係数の列とみなして、定義多項式 $F=Y^3+X^4+7X$ を生成する。

【 0 1 0 9 】

次に、イデアル縮約部13は、前記単項式のリスト1, X, Y, X², X Y, Y², X³中のそれぞれのM_i (1≤i≤7)に対して、M_iと多項式gの積M_i gの、多項式fおよびFによる剰余式r_iを計算し、その係数を、代数曲線パラメータファイルAの単項式順序1, X, Y, . . . の順にならべて、ベクトルw⁽ⁱ⁾₁を生成する。さらに、M_iと多項式hの積M_i hの、多項式fおよびFによる剰余式s_iを計算し、その係数を、代数曲線パラメータファイルAの単項式順序1, X, Y, . . . の順にならべて、ベクトルw⁽ⁱ⁾₂を生成し、上記2つのベクトルw⁽ⁱ⁾₁とw⁽ⁱ⁾₂を連結してベクトルv_iを生成する。

【0 1 1 0】

すなわち、まず、第一番目の単項式M₁=1に対して、 $1 \cdot g = 449 + 79 X + 320 Y + X Y$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 449 + 79 X + 320 Y + X Y$ となるので、剰余 $449 + 79 X + 320 Y + X Y$ を得て、ベクトルw⁽¹⁾₁=(449, 79, 320, 1, 0, 0)を生成する。また、 $1 \cdot h=544 + 564 X + 195 Y + Y^2$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $h = 0 \cdot f + 0 \cdot F + 544 + 564 X + 195 Y + Y^2$ となるので、剰余 $544 + 564 X + 195 Y + Y^2$ を得て、ベクトルw⁽¹⁾₂=(544, 564, 195, 0, 1, 0)を生成する。そして、ベクトルw⁽¹⁾₁とw⁽¹⁾₂を連結して、ベクトルv₁=(449, 79, 320, 1, 0, 0, 544, 564, 195, 0, 1, 0)を得る。

【0 1 1 1】

次に、第二番目の単項式M₂=Xに対して、 $X g = X (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X g = (79 + Y) f + 0 \cdot F + 115 + 757 X + 601 Y + 94 X Y + 863 Y^2$ となるので、剰余 $115 + 757 X + 601 Y + 94 X Y + 863 Y^2$ を得て、ベクトルw⁽²⁾₁=(115, 757, 601, 94, 863, 0)を生成する。

【0 1 1 2】

また、 $X h=X (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X h = 564 f + 0 \cdot F + 93 + 214 X + 394 Y + 195 X Y + X Y^2$ となるので、剰余 $93 + 214 X + 394 Y + 195 X Y + X Y^2$ を得て、ベクトルw⁽²⁾₂=(93, 214, 394, 195, 0, 1)を生成する。そして、ベクトルw⁽²⁾₁とw⁽²⁾₂を

連結して、ベクトル $v_2=(115, 757, 601, 94, 863, 0, 93, 214, 394, 195, 0, 1)$ を得る。

【 0 1 1 3 】

次に、第三番目の単項式 $M_3=Y$ に対して、 $Y g = Y (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $Y g = 0 \cdot f + 0 \cdot F + 449 Y + 79 X Y + 320 Y^2 + X Y^2$ となるので、剰余 $449 Y + 79 X Y + 320 Y^2 + X Y^2$ を得て、ベクトル $w^{(3)}_1=(0, 0, 449, 79, 320, 1)$ を生成する。

【 0 1 1 4 】

また、 $Y h = Y (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $Y h = (356 + 226 X + 1008 X^2 + 146 Y) f + 1 \cdot F + 531 + 305 X + 942 Y + 157 X Y + 68 Y^2$ となるので、剰余 $531 + 305 X + 942 Y + 157 X Y + 68 Y^2$ を得て、ベクトル $w^{(3)}_2=(531, 305, 942, 157, 68, 0)$ を生成する。そして、ベクトル $w^{(3)}_1$ と $w^{(3)}_2$ を連結して、ベクトル $v_3=(0, 0, 449, 79, 320, 1, 531, 305, 942, 157, 68, 0)$ を得る。

【 0 1 1 5 】

次に、第四番目の単項式 $M_4=X^2$ に対して、 $X^2 g = X^2 (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X^2 g = (757 + 79 X + 94 Y + X Y) f + 0 \cdot F + 259 + 563 X + 988 Y + 546 X Y + 402 Y^2 + 863 X Y^2$ となるので、剰余 $259 + 563 X + 988 Y + 546 X Y + 402 Y^2 + 863 X Y^2$ を得て、ベクトル $w^{(4)}_1=(259, 563, 988, 546, 402, 863)$ を生成する。

【 0 1 1 6 】

また、 $X^2 h = X^2 (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X^2 h = (706 + 865 X + 146 X^2 + 68 Y + Y^2) f + 863 F + 900 + 27 X + 669 Y + 611 X Y + 189 Y^2 + 783 X Y^2$ となるので、剰余 $900 + 27 X + 669 Y + 611 X Y + 189 Y^2 + 783 X Y^2$ を得て、ベクトル $w^{(4)}_2=(900, 27, 669, 611, 189, 783)$ を生成する。そして、ベクトル $w^{(4)}_1$ と $w^{(4)}_2$ を連結して、ベクトル $v_4=(259, 563, 988, 546, 402, 863, 900, 27, 669, 611, 189, 783)$ を得る。

【 0 1 1 7 】

次に、第五番目の単項式 $M_5 = X Y$ に対して、 $X Y g = X Y (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X Y g = (492 + 301 X + 146 X^2 + 961 Y + Y^2) f + 863 F + 167 + 875 X + 529 Y + 648 X Y + 981 Y^2 + 94 X Y^2$ となるので、剰余 $167 + 875 X + 529 Y + 648 X Y + 981 Y^2 + 94 X Y^2$ を得て、ベクトル $w^{(5)}_1 = (167, 875, 529, 648, 981, 94)$ を生成する。

【 0 1 1 8 】

また、 $X Y h = X Y (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X Y h = (305 + 356 X + 226 X^2 + 1008 X^3 + 157 Y + 146 X Y) f + X F + 163 + 213 X + 69 Y + 775 X Y + 285 Y^2 + 68 X Y^2$ となるので、剰余 $163 + 213 X + 69 Y + 775 X Y + 285 Y^2 + 68 X Y^2$ を得て、ベクトル $w^{(5)}_2 = (163, 213, 69, 775, 285, 68)$ を生成する。そして、ベクトル $w^{(5)}_1$ と $w^{(5)}_2$ を連結して、ベクトル $v_5 = (167, 875, 529, 648, 981, 94, 163, 213, 69, 775, 285, 68)$ を得る。

【 0 1 1 9 】

次に、第六番目の単項式 $M_6 = Y^2$ に対して、 $Y^2 g = Y^2 (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $Y^2 g = (208 + 28 X + 915 X^2 + 1008 X^3 + 908 Y + 146 X Y) f + (320 + X) F + 571 + 949 X + 202 Y + 482 X Y + 60 Y^2 + 961 X Y^2$ となるので、剰余 $571 + 949 X + 202 Y + 482 X Y + 60 Y^2 + 961 X Y^2$ を得て、ベクトル $w^{(6)}_1 = (571, 949, 202, 482, 60, 961)$ を生成する。

【 0 1 2 0 】

また、 $Y^2 h = Y^2 (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $Y^2 h = (1001 + 233 X + 941 X^2 + 194 Y + 226 X Y + 1008 X^2 Y + 146 Y^2) f + (68 + Y) F + 793 + 560 X + 352 Y + 881 X Y + 378 Y^2 + 157 X Y^2$ となるので、剰余 $793 + 560 X + 352 Y + 881 X Y + 378 Y^2 + 157 X Y^2$ を得て、ベクトル $w^{(6)}_2 = (793, 560, 352, 881, 378, 157)$ を生成する。そして、ベクトル $w^{(6)}_1$ と $w^{(6)}_2$ を連結して、ベクトル $v_6 = (571, 949, 202, 482, 60, 961, 793, 560, 352, 881, 378, 157)$ を得る。

【0 1 2 1】

最後に、第七番目の単項式 $M_7 = X^3$ に対して、 $X^3 g = X^3 (449 + 79 X + 320 Y + X Y)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X^3 g = (370 + 198 X + 961 X^2 + 926 Y + 94 X Y + X^2 Y + 863 Y^2) f + 127 F + 909 + 548 X + 243 Y + 460 X Y + 104 Y^2 + 101 X Y^2$ となるので、剰余 $909 + 548 X + 243 Y + 460 X Y + 104 Y^2 + 101 X Y^2$ を得て、ベクトル $w^{(7)}_1 = (909, 548, 243, 460, 104, 101)$ を生成する。

【0 1 2 2】

また、 $X^3 h = X^3 (544 + 564 X + 195 Y + Y^2)$ を $f=982 + 226 X + 146 Y + X^2$ および $F=Y^3+X^4+7X$ で割ると、 $X^3 h = (834 + 283 X + 157 X^2 + 146 X^3 + 52 Y + 68 X Y + 783 Y^2 + X Y^2) f + (708 + 863 X) F + 320 + 866 X + 720 Y + 225 X Y + 432 Y^2 + 815 X Y^2$ となるので、剰余 $320 + 866 X + 720 Y + 225 X Y + 432 Y^2 + 815 X Y^2$ を得て、ベクトル $w^{(7)}_2 = (320, 866, 720, 225, 432, 815)$ を生成する。そして、ベクトル $w^{(7)}_1$ と $w^{(7)}_2$ を連結して、ベクトル $v_7 = (909, 548, 243, 460, 104, 101, 320, 866, 720, 225, 432, 815)$ を得る。以上で、第二のイデアル縮約部13の多項式ベクトル生成部32における処理を終了する。

【0 1 2 3】

次に、第二のイデアル部装置13は、基底構成部33において、多項式ベクトル生成部32で生成した、7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を線形関係導出部34に入力し、出力として複数の7次元ベクトル m_1, m_2, \dots を得る。線形関係導出部34は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術に属するので、以下、線形関係導出部34の動作はその概略のみ示す。

【0 1 2 4】

線形関係導出部34は、まず、入力された7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を順に並べて 7×12 行列

【数 1 7】

$$M_R = \begin{pmatrix} 449 & 79 & 320 & 1 & 0 & 0 & 544 & 564 & 195 & 0 & 1 & 0 \\ 115 & 757 & 601 & 94 & 863 & 0 & 93 & 214 & 394 & 195 & 0 & 1 \\ 0 & 0 & 449 & 79 & 320 & 1 & 531 & 305 & 942 & 157 & 68 & 0 \\ 259 & 563 & 988 & 546 & 402 & 863 & 900 & 27 & 669 & 611 & 189 & 783 \\ 167 & 875 & 529 & 648 & 981 & 94 & 163 & 213 & 69 & 775 & 285 & 68 \\ 571 & 949 & 202 & 482 & 60 & 961 & 793 & 560 & 352 & 881 & 378 & 157 \\ 909 & 548 & 243 & 460 & 104 & 101 & 320 & 866 & 720 & 225 & 432 & 815 \end{pmatrix}$$

を構成する。

【 0 1 2 5】

次に、線形関係導出装置34は、行列 M_R に7次元の単位行列を連結し、

【数 1 8】

$$M'_R = \begin{pmatrix} 449 & 79 & 320 & 1 & 0 & 0 & 544 & 564 & 195 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 757 & 601 & 94 & 863 & 0 & 93 & 214 & 394 & 195 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 449 & 79 & 320 & 1 & 531 & 305 & 942 & 157 & 68 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 259 & 563 & 988 & 546 & 402 & 863 & 900 & 27 & 669 & 611 & 189 & 783 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 167 & 875 & 529 & 648 & 981 & 94 & 163 & 213 & 69 & 775 & 285 & 68 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 571 & 949 & 202 & 482 & 60 & 961 & 793 & 560 & 352 & 881 & 378 & 157 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 909 & 548 & 243 & 460 & 104 & 101 & 320 & 866 & 720 & 225 & 432 & 815 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

を構成する。

【 0 1 2 6】

次に、線形関係導出装置34は、 i 行目の定数倍を $i+1$ 行目から7行目に加えること
で($i=1, 2, 3$)、行列 M'_R を三角化し以下の行列 m を得る。

第13成分以降よりなるベクトル $m_3=(394, 852, 48, 0, 0, 1, 0)$ および行列 m の7行目の第13成分以降よりなるベクトル $m_4=(382, 194, 908, 0, 0, 0, 1)$ を出力する。

【 0 1 2 8 】

第二のイデアル縮約部13の基底構成部33における処理の説明に戻る。次に、第二のイデアル縮約部13は、図7のグレブナ基底構成用テーブル37を参照し前記値 $d=3$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(982, 226, 146, 1, 0, 0, 0)$ 、 $m_2=(53, 941, 915, 0, 1, 0, 0)$ 、 $m_3=(394, 852, 48, 0, 0, 1, 0)$ および $m_4=(382, 194, 908, 0, 0, 0, 1)$ 中に存在しないレコードを検索する。第14レコードの位数フィールドの値は3であり、第14レコードの成分番号リスト4,5,6,7に対応する成分がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第14レコードが得られる。

【 0 1 2 9 】

さらに第14レコードの第一ベクトル型の値は $(*, *, *, 1, 0, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(982, 226, 146, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_1=982 + 226 X + 146 Y + X^2$ を生成する。

【 0 1 3 0 】

同様にして、第14レコードの第二ベクトル型の値は $(*, *, *, 0, 1, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(53, 941, 915, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, Y, X^2 , X Y, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_2=53 + 941 X + 915 Y + X Y$ を生成する。

【 0 1 3 1 】

同様にして、第14レコードの第三ベクトル型の値は $(*, *, *, 0, 0, 1, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_3=(394, 852, 48, 0, 0, 1, 0)$ と合致するので、ベクトル m_3 を、代数曲線パラメータファイルAの単項式順序

1, X , Y , X^2 , $X Y$, Y^2 , X^3 の各単項式の係数の列とみなし、多項式 $f_3=394 + 852 X + 48 Y + Y^2$ を生成する。最後に、イデアル縮約装置13は、多項式の集合 $J^{**}=\{f_1=982 + 226 X + 146 Y + X^2, f_2=53 + 941 X + 915 Y + X Y, f_3=394 + 852 X + 48 Y + Y^2\}$ を構成し、出力する。以上で、第二のイデアル縮約部13の動作は終了する。

【 0 1 3 2 】

最後に、図1のヤコビ群加算装置において、第二のイデアル縮約部13の出力したグレブナ基底 $J^{**}=\{982 + 226 X + 146 Y + X^2, 53 + 941 X + 915 Y + X Y, 394 + 852 X + 48 Y + Y^2\}$ が出力装置より出力される。

次に、 C_{27} 曲線を用いた場合の実施例を示す。本実施例では、代数曲線パラメータファイルとして図8の代数曲線パラメータファイルを、イデアル型テーブルとして図9のイデアル型テーブルを、単項式ストテーブルとして図10の単項式リストテーブルを、グレブナ基底構成用テーブルとして図11のグレブナ基底構成用テーブルを用いる。

【 0 1 3 3 】

図1のヤコビ群要素加算装置において、図8の代数曲線パラメータファイルAおよび代数曲線パラメータファイルA で指定された C_{27} 曲線のヤコビ群の要素を表す、代数曲線パラメータファイルAで指定された代数曲線の座標環のイデアルのグレブナ基底

$$I_1 = \{689 + 623 X + 130 X^2 + X^3, 568 + 590 X + 971 X^2 + Y\}$$

および

$$I_2 = \{689 + 623 X + 130 X^2 + X^3, 568 + 590 X + 971 X^2 + Y\}$$

が入力されたとする。

【 0 1 3 4 】

まず、イデアル合成部11が、図2に示す機能ブロックの処理の流れにしたがって、図8の代数曲線パラメータファイルA、上記グレブナ基底 I_1 および I_2 を入力として以下のように動作する。イデアル合部11は、まず、図2のイデアル型分類部21において、図9のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル I_1 の型と一致するレコードを検索し第11レコ

ードを得て、第11レコードのイデアル型番号フィールドの値 $N_1=31$ および位数フィールドの値 $d_1=3$ を取得する。同様に、イデアル型が入力イデアル I_2 の型と一致するレコードを検索し第11レコードを得て、第11レコードのイデアル型番号フィールドの値 $N_2=31$ および位数フィールドの値 $d_2=3$ を取得する。

【 0 1 3 5 】

次に、イデアル合成部11は、単項式ベクトル生成部22において、前記位数フィールドの値 $d_1=3$ および $d_2=3$ の和 $d_3=d_1+d_2=6$ を計算し、単項式リストテーブルを参照し前記 $d_3=6$ を位数フィールドの値に持つレコードを検索し第1レコードを得て、第1レコードの単項式リストフィールドに記述されている単項式のリスト1, X , X^2 , X^3 , Y , X^4 , XY , X^5 , $X^2 Y$, X^6 を取得する。 I_1 と I_2 は同一なので、前記単項式のリスト1, X , X^2 , X^3 , Y , X^4 , XY , X^5 , $X^2 Y$, X^6 中のそれぞれの M_i ($1 \leq i \leq 10$) に対して、 M_i を I_1 で割った剰余を計算し、多項式 $a^{(i)}_1 + a^{(i)}_2 X + a^{(i)}_3 X^2$ を得て、その係数を、代数曲線パラメータファイルAの単項式順序1, X , X^2 , ... の順にならべて、ベクトル $w^{(i)}_1 = (a^{(i)}_1, a^{(i)}_2, a^{(i)}_3)$ を生成する。

【 0 1 3 6 】

さらに、図8の代数曲線パラメータファイルAに記述された係数リスト0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1を、図8の代数曲線パラメータファイルAに記述された単項式順序1, X , X^2 , X^3 , Y , X^4 , XY , X^5 , $X^2 Y$, X^6 , $X^3 Y$, X^7 , Y^2 の各単項式の係数列とみなし、定義多項式 $F=Y^2 + X^7 + 7 X$ を構成し、多項式 M に対してその X による微分を $D_X(M)$ 、 Y による微分を $D_Y(M)$ と書くとき、多項式 $D_X(M_i) D_Y(F) - D_Y(M_i) D_X(F)$ を I_1 で割った剰余を計算し、多項式 $b^{(i)}_1 + b^{(i)}_2 X + b^{(i)}_3 X^2$ を得て、その係数を、代数曲線パラメータファイルAの単項式順序1, X , X^2 , ... の順にならべて、ベクトル $w^{(i)}_2 = (b^{(i)}_1, b^{(i)}_2, b^{(i)}_3)$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル $v_i = (a^{(i)}_1, a^{(i)}_2, a^{(i)}_3, b^{(i)}_1, b^{(i)}_2, b^{(i)}_3)$ を生成する。すなわち、 $M_1 = 1$ を I_1 でわると、 $1 = 0 \cdot (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 1$ となるので、剰余として1を得て、ベクトル $w^{(1)}_1 = (1, 0, 0)$ を生成する。さらに、 $D_X(1) D_Y(F) - D_Y(1) D_X(F) = 0$ を I_1 で割ると、0となるので、剰余として0を得て、ベクトル $w^{(1)}_2 = (0, 0, 0)$ を生成する。 $w^{(1)}_1$ と $w^{(1)}_2$ を連結して、ベクトル $v_1 = (1, 0, 0, 0, 0, 0)$ を生成する。

【0 1 3 7】

次に、 $M_2 = X$ を I_1 でわると、 $X = 0 \cdot (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + X$ となるので、剰余として X を得て、ベクトル $w^{(2)}_1 = (0, 1, 0)$ を生成する。さらに、 $D_X(X)D_Y(F) - D_Y(X)D_X(F) = D_Y(F) = 2 Y$ を I_1 でわると、 $2 Y = 0 \cdot (689 + 623 X + 130 X^2 + X^3) + 2 (568 + 590 X + 971 X^2 + Y) + 882 + 838 X + 76 X^2$ となるので、剰余として $882 + 838 X + 76 X^2$ を得て、ベクトル $w^{(2)}_2 = (882, 838, 76)$ を生成する。 $w^{(2)}_1$ と $w^{(2)}_2$ を連結して、ベクトル $v_2 = (0, 1, 0, 882, 838, 76)$ を生成する。

【0 1 3 8】

次に、 $M_3 = X^2$ を I_1 でわると、 $X^2 = 0 \cdot (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + X^2$ となるので、剰余として X^2 を得て、ベクトル $w^{(3)}_1 = (0, 0, 1)$ を生成する。さらに、 $D_X(X^2)D_Y(F) - D_Y(X^2)D_X(F) = 4 X Y$ を I_1 でわると、 $4 X Y = 152 (689 + 623 X + 130 X^2 + X^3) + 4 X (568 + 590 X + 971 X^2 + Y) + 208 + 905 X + 78 X^2$ となるので、剰余として $208 + 905 X + 78 X^2$ を得て、ベクトル $w^{(3)}_2 = (208, 905, 78)$ を生成する。 $w^{(3)}_1$ と $w^{(3)}_2$ を連結して、ベクトル $v_3 = (0, 0, 1, 208, 905, 78)$ を生成する。

【0 1 3 9】

次に、 $M_4 = X^3$ を I_1 でわると、 $X^3 = 1 \cdot (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 320 + 386 X + 879 X^2$ となるので、剰余として $320 + 386 X + 879 X^2$ を得て、ベクトル $w^{(4)}_1 = (320, 386, 879)$ を生成する。さらに、 $D_X(X^3)D_Y(F) - D_Y(X^3)D_X(F) = 6 X^2 Y$ を I_1 でわると、 $6 X^2 Y = (117 + 228 X) (689 + 623 X + 130 X^2 + X^3) + 6 X^2 (568 + 590 X + 971 X^2 + Y) + 107 + 69 X + 778 X^2$ となるので、剰余として $107 + 69 X + 778 X^2$ を得て、ベクトル $w^{(4)}_2 = (107, 69, 778)$ を生成する。 $w^{(4)}_1$ と $w^{(4)}_2$ を連結して、ベクトル $v_4 = (320, 386, 879, 107, 69, 778)$ を生成する。

【0 1 4 0】

次に、 $M_5 = Y$ を I_1 でわると、 $Y = 0 \cdot (689 + 623 X + 130 X^2 + X^3) + 1 \cdot (568 + 590 X + 971 X^2 + Y) + 441 + 419 X + 38 X^2$ となるので、剰余として $441 + 419 X + 38 X^2$ を得て、ベクトル $w^{(5)}_1 = (441, 419, 38)$ を生成する。さらに、 $D_X(Y)D$

$Y(F) \cdot -D_Y(Y)D_X(F) = -D_X(F) = 1002 + 1002 X^6$ を I_1 でわると、 $1002 + 1002 X^6 = (865 + 78 X + 910 X^2 + 1002 X^3) (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 327 + 655 X + 1004 X^2$ となるので、剰余として $327 + 655 X + 1004 X^2$ を得て、ベクトル $w^{(5)}_2 = (327, 655, 1004)$ を生成する。 $w^{(5)}_1$ と $w^{(5)}_2$ を連結して、ベクトル $v_5 = (441, 419, 38, 327, 655, 1004)$ を生成する。

【 0 1 4 1 】

次に、 $M_6 = X^4$ を I_1 でわると、 $X^4 = (879 + X) (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 778 + 590 X + 133 X^2$ となるので、剰余として $778 + 590 X + 133 X^2$ を得て、ベクトル $w^{(6)}_1 = (778, 590, 133)$ を生成する。さらに、 $D_X(X^4)D_Y(F) - D_Y(X^4)D_X(F) = 8 X^3 Y$ を I_1 でわると、 $8 X^3 Y = (200 + 840 X + 8 Y) (689 + 623 X + 130 X^2 + X^3) + (542 + 61 X + 978 X^2) (568 + 590 X + 971 X^2 + Y) + 322 + 653 X + 781 X^2$ となるので、剰余として $322 + 653 X + 781 X^2$ を得て、ベクトル $w^{(6)}_2 = (322, 653, 781)$ を生成する。 $w^{(6)}_1$ と $w^{(6)}_2$ を連結して、ベクトル $v_6 = (778, 590, 133, 322, 653, 781)$ を生成する。

【 0 1 4 2 】

次に、 $M_7 = X Y$ を I_1 でわると、 $X Y = 38 (689 + 623 X + 130 X^2 + X^3) + X (568 + 590 X + 971 X^2 + Y) + 52 + 983 X + 524 X^2$ となるので、剰余として $52 + 983 X + 524 X^2$ を得て、ベクトル $w^{(7)}_1 = (52, 983, 524)$ を生成する。さらに、 $D_X(X Y)D_Y(F) - D_Y(X Y)D_X(F) = 1002 X + 1002 X^7 + 2 Y^2$ を I_1 でわると、 $1002 X + 1002 X^7 + 2 Y^2 = (24 + 726 X + 78 X^2 + 910 X^3 + 1002 X^4) (689 + 623 X + 130 X^2 + X^3) + (882 + 838 X + 76 X^2 + 2 Y) (568 + 590 X + 971 X^2 + Y) + 105 + 954 X + 813 X^2$ となるので、剰余として $105 + 954 X + 813 X^2$ を得て、ベクトル $w^{(7)}_2 = (105, 954, 813)$ を生成する。 $w^{(7)}_1$ と $w^{(7)}_2$ を連結して、ベクトル $v_7 = (52, 983, 524, 105, 954, 813)$ を生成する。

【 0 1 4 3 】

次に、 $M_8 = X^5$ を I_1 でわると、 $X^5 = (133 + 879 X + X^2) (689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 182 + 657 X + 453 X^2$ となるので、剰余として $182 + 657 X + 453 X^2$ を得て、ベクトル $w^{(8)}_1 = (182, 657, 453)$ を生成する。さらに、 $D_X(X^5)D_Y(F) - D_Y(X^5)D_X(F) = 10 X^4 Y$ を I_1 でわると、 $10 X^4 Y =$

$(912 + 90 X + 718 Y + 10 X Y)(689 + 623 X + 130 X^2 + X^3) + (717 + 855 X + 321 X^2)(568 + 590 X + 971 X^2 + Y) + 619 + 878 X + 281 X^2$ となるので、剰余として $619 + 878 X + 281 X^2$ を得て、ベクトル $w(8)_2 = (619, 878, 281)$ を生成する。 $w(8)_1$ と $w(8)_2$ を連結して、ベクトル $v_8 = (182, 657, 453, 619, 878, 281)$ を生成する。

【 0 1 4 4 】

次に、 $M_9 = X^2 Y$ を I_1 でわると、 $X^2 Y = (524 + 38 X)(689 + 623 X + 130 X^2 + X^3) + X^2(568 + 590 X + 971 X^2 + Y) + 186 + 516 X + 466 X^2$ となるので、剰余として $186 + 516 X + 466 X^2$ を得て、ベクトル $w(9)_1 = (186, 516, 466)$ を生成する。さらに、 $DX(X^2 Y)DY(F) - DY(X^2 Y)DX(F) = 1002 X^2 + 1002 X^8 + 4 X Y^2$ を I_1 でわると、 $1002 X^2 + 1002 X^8 + 4 X Y^2 = (892 + 941 X + 865 X^2 + 78 X^3 + 910 X^4 + 1002 X^5 + 152 Y)(689 + 623 X + 130 X^2 + X^3) + (208 + 905 X + 78 X^2 + 4 X Y)(568 + 590 X + 971 X^2 + Y) + 811 + 600 X + 123 X^2$ となるので、剰余として $811 + 600 X + 123 X^2$ を得て、ベクトル $w(9)_2 = (811, 600, 123)$ を生成する。 $w(9)_1$ と $w(9)_2$ を連結して、ベクトル $v_9 = (186, 516, 466, 811, 600, 123)$ を生成する。

【 0 1 4 5 】

次に、 $M_{10} = X^6$ を I_1 でわると、 $X^6 = (453 + 133 X + 879 X^2 + X^3)(689 + 623 X + 130 X^2 + X^3) + 0 \cdot (568 + 590 X + 971 X^2 + Y) + 673 + 483 X + 289 X^2$ となるので、剰余として $673 + 483 X + 289 X^2$ を得て、ベクトル $w(10)_1 = (673, 483, 289)$ を生成する。さらに、 $DX(X^6)DY(F) - DY(X^6)DX(F) = 12 X^5 Y$ を I_1 でわると、 $12 X^5 Y = (985 + 732 X + 587 Y + 458 X Y + 12 X^2 Y)(689 + 623 X + 130 X^2 + X^3) + (166 + 821 X + 391 X^2)(568 + 590 X + 971 X^2 + Y) + 950 + 741 X + 201 X^2$ となるので、剰余として $950 + 741 X + 201 X^2$ を得て、ベクトル $w(10)_2 = (950, 741, 201)$ を生成する。 $w(10)_1$ と $w(10)_2$ を連結して、ベクトル $v_{10} = (673, 483, 289, 950, 741, 201)$ を生成する。以上で、イデアル合成部11の単項式ベクトル生成部22における処理を終了する。

【 0 1 4 6 】

次に、イデアル合成部11は、基底構成部23において、単項式ベクトル生成部22で

生成した、10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ を線形関係導出部24に入力し、出力として複数の10次元ベクトル m_1, m_2, \dots を得る。線形関係導出部24は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術であるので、以下、線形関係導出部24の動作はその概略のみ示す。線形関係導出部24は、まず、入力された10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ を順に並べて10x6行列

【数 2 0】

$$M_c = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 882 & 838 & 76 \\ 0 & 0 & 1 & 208 & 905 & 78 \\ 320 & 386 & 879 & 107 & 69 & 778 \\ 441 & 419 & 38 & 327 & 655 & 1004 \\ 778 & 590 & 133 & 322 & 653 & 781 \\ 52 & 983 & 524 & 105 & 954 & 813 \\ 182 & 657 & 453 & 619 & 878 & 281 \\ 186 & 516 & 466 & 811 & 600 & 123 \\ 673 & 483 & 289 & 950 & 741 & 201 \end{pmatrix}$$

を構成する。

【0 1 4 7】

次に、線形関係導出装置24は、行列 M_c に10次元の単位行列を連結し、

【数 2 1】

$$M'_c = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 882 & 838 & 76 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 208 & 905 & 78 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 320 & 386 & 879 & 107 & 69 & 778 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 441 & 419 & 38 & 327 & 655 & 1004 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 778 & 590 & 133 & 322 & 653 & 781 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 52 & 983 & 524 & 105 & 954 & 813 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 182 & 657 & 453 & 619 & 878 & 281 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 186 & 516 & 466 & 811 & 600 & 123 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 673 & 483 & 289 & 950 & 741 & 201 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

を得る。

次に、線形関係導出部24は、 i 行目の定数倍を $i+1$ 行目から10行目に加える事で($i=1, 2, \dots, 6$)、行列 M'_c を三角化し以下の行列 m を得る。

【0 1 4 8】

【数 2 2】

$$m = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 882 & 838 & 76 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 208 & 905 & 78 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 494 & 87 & 753 & 689 & 623 & 130 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 477 & 924 & 591 & 170 & 804 & 22 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 475 & 742 & 22 & 242 & 149 & 314 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 699 & 601 & 688 & 281 & 217 & 287 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 193 & 959 & 364 & 180 & 550 & 43 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 780 & 667 & 96 & 50 & 897 & 327 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 761 & 727 & 417 & 523 & 278 & 912 & 0 & 0 & 0 & 1 \end{pmatrix}$$

よく知られているように行列 m の7から10行目の第7成分以降よりなるベクトルは、入力された10個の6次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}$ の全ての1次独立な線形従属関係 $\sum_{i=1}^{10} m_{ji} v_i = 0$ ($j=1, 2, \dots$)を表すベクトル $\{(m_1, 1, m_1, 2, \dots, m_1, n), (m_2, 1, m_2, 2, \dots, m_2, n), \dots\}$ である。線形関係導出部24は、行列 m の7行目の第7成分以降よりなるベクトル $m_1=(699, 601, 688, 281, 217, 287, 1, 0, 0, 0)$ 、行列 m の8行目の第7成分以降よりなるベクトル $m_2=(193, 959, 364, 180, 550, 43, 0, 1, 0, 0)$ 、行列 m の9行目の第7成分以降よりなるベクトル $m_3=(780, 667, 96, 50, 897, 327, 0, 0, 1, 0)$ および行列 m の10行目の第7成分以降よりなるベクトル $m_4=(761, 727, 417, 523, 278, 912, 0, 0, 0, 1)$ を出力する。イデアル合成部11の基底構成部23における処理の説明に戻る。

【0 1 4 9】

次に、イデアル合成部11は、図11のグレブナ基底構成用テーブルを参照し前記値 $d_3=6$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(699, 601, 688, 281, 217, 287, 1, 0, 0, 0)$ 、 $m_2=(193, 959, 364, 180, 550, 43, 0, 1, 0, 0)$ 、 $m_3=(780, 667, 96, 50, 897, 327, 0, 0, 1, 0)$ および $m_4=(761, 727, 417, 523, 278, 912, 0, 0, 0, 1)$

中に存在しないレコードを検索する。第1レコードの位数フィールドの値は6であり、第1レコードの成分番号リスト7, 8, 9, 10に対応する成分がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第1レコードが得られる。

【0 1 5 0】

さらに第1レコードの第一ベクトル型の値は(*, *, *, *, *, *, 1, 0, 0, 0)であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1 = (699, 601, 688, 281, 217, 287, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , X^3 , Y, X^4 , XY, X^5 , $X^2 Y$, X^6 の各単項式の係数の列とみなし、多項式 $f_1 = 699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ を生成する。

【0 1 5 1】

同様にして、第1レコードの第二ベクトル型の値は(*, *, *, *, *, *, 0, 1, 0, 0)であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2 = (193, 959, 364, 180, 550, 43, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , X^3 , Y, X^4 , XY, X^5 , $X^2 Y$, X^6 の各単項式の係数の列とみなし、多項式 $f_2 = 193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5$ を生成する。第1レコードの第三ベクトル型の値はnullなので、無視される。最後に、イデアル合成部11は、多項式の集合 $J = \{f_1, f_2\} = \{699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY, 193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5\}$ を構成し、出力する。以上で、イデアル合成部11の動作は終了する。

【0 1 5 2】

次に、第一のイデアル縮約部12が、図3に示す機能ブロックの処理の流れにしたがって、図8の代数曲線パラメータファイルAおよびイデアル合成部11が出力したグレブナ基底

$$J = \{699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + X Y, 193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5\}$$

を入力として以下のように動作する。

【0 1 5 3】

まず、イデアル縮約部12は、図3のイデアル型分類部31において、図9のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアルJの型と一致するレコードを検索し第1レコードを得て、第1レコードのイデアル型番号フィールドの値N=61および縮約位数フィールドの値d=3を取得する。次に、イデアル縮約部12は、前記d=3が0でないことを確認し、多項式ベクトル生成部32において、図10の単項式リストテーブルを参照し前記d=3を位数フィールドの値に持つレコードを検索し第4レコードを得て、第4レコードの単項式リストフィールドに記述されている単項式のリスト1, X, X², X³, Y, X⁴, XYを取得する。

【0 1 5 4】

さらに、イデアル縮約部12は、

Jの第1要素 $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ 、第2要素 $g=193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5$ を取得し(Jには第3要素はないので第3番目の多項式hは用いない)、代数曲線パラメータファイルAの係数リスト0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1を、代数曲線パラメータファイルAの単項式順序1, X, X², X³, Y, X⁴, XY, X⁵, X² Y, X⁶, X³ Y, X⁷, Y²の各単項式の係数の列とみなして、定義多項式 $F=Y^2+X^7+7X$ を生成する。

【0 1 5 5】

次に、イデアル縮約部12は、前記単項式のリスト1, X, X², X³, Y, X⁴, XY中のそれぞれの M_i ($1 \leq i \leq 7$) に対して、 M_i と多項式gの積 $M_i \cdot g$ の、多項式fおよびFによる剰余式 r_i を計算し、その係数を、代数曲線パラメータファイルAの単項式順序1, X, X², X³, Y, X⁴, XY, X⁵, X² Y, X⁶, X³ Y, X⁷の順にならべて、ベクトル v_i を生成する。すなわち、まず、第一番目の単項式 $M_1=1$ に対して、 $1 \cdot g = 193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F=Y^2+X^7+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5$ となるので、剰余 $193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5$ を得て、ベクトル $v_1=(193, 959, 364, 180, 550, 43, 0, 1, 0, 0, 0, 0, 0)$ を生成する。

【0 1 5 6】

次に、第二番目の単項式 $M_2=X$ に対して、 $X g = X (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F= Y^2+X^7+7X$ で割ると、 $X g = 550 f + 0 \cdot F + 988 + 595 X + 934 X^2 + 191 X^3 + 743 X^4 + 43 X^5 + X^6 + 721 Y$ となるので、剰余 $988 + 595 X + 934 X^2 + 191 X^3 + 743 X^4 + 43 X^5 + X^6 + 721 Y$ を得て、ベクトル $v_2=(988, 595, 934, 191, 721, 743, 0, 43, 0, 1, 0, 0)$ を生成する。

【0 1 5 7】

次に、第三番目の単項式 $M_3=X^2$ に対して、 $X^2 g = X^2 (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F= Y^2+X^7+7X$ で割ると、 $X^2 g = (721 + 550 X) f + 0 \cdot F + 521 + 528 X + 975 X^2 + 133 X^3 + 109 X^4 + 743 X^5 + 43 X^6 + X^7 + 947 Y$ となるので、剰余 $521 + 528 X + 975 X^2 + 133 X^3 + 109 X^4 + 743 X^5 + 43 X^6 + X^7 + 947 Y$ を得て、ベクトル $v_3=(521, 528, 975, 133, 947, 109, 0, 743, 0, 43, 0, 1)$ を生成する。

【0 1 5 8】

次に、第四番目の単項式 $M_4=X^3$ に対して、 $X^3 g = X^3 (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F= Y^2+X^7+7X$ で割ると、 $X^3 g = (200 + 969 X + 101 X^2 + 287 X^3 + 1008 Y) f + (217 + X) F + 451 + 78 X + 481 X^2 + 791 X^3 + 389 X^4 + 924 X^5 + 527 X^6 + 195 X^7 + 686 Y$ となるので、剰余 $451 + 78 X + 481 X^2 + 791 X^3 + 389 X^4 + 924 X^5 + 527 X^6 + 195 X^7 + 686 Y$ を得て、ベクトル $v_4=(451, 78, 481, 791, 686, 389, 0, 924, 0, 527, 0, 195)$ を生成する。

【0 1 5 9】

次に、第五番目の単項式 $M_5=Y$ に対して、 $Y g = Y (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F= Y^2+X^7+7X$ で割ると、 $Y g = (884 + 712 X + 316 X^2 + 195 X^3 + X^4 + 287 Y) f + (829 + 722 X) F + 601 + 459 X + 217 X^2 + 14 X^3 + 965 X^4 + 924 X^5 + 130 X^6 + 438 X^7 + 253 Y$ となるので、剰余 $601 + 459 X + 217 X^2 +$

$14 X^3 + 965 X^4 + 924 X^5 + 130 X^6 + 438 X^7 + 253 Y$ を得て、ベクトル $v_5=(601, 459, 217, 14, 253, 965, 0, 924, 0, 130, 0, 438)$ を生成する。

【 0 1 6 0 】

次に、第六番目の単項式 $M_6=X^4$ に対して、 $X^4 g = X^4 (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F=Y^2+X^7+7X$ で割ると、 $X^4 g = (317 + 128 X + 188 X^2 + 571 X^3 + 287 X^4 + 814 Y + 1008 X Y) f + (946 + 412 X + X^2) F + 397 + 954 X + 514 X^2 + 891 X^3 + 255 X^4 + 901 X^5 + 173 X^6 + 906 X^7 + 922 Y$ となるので、剰余 $397 + 954 X + 514 X^2 + 891 X^3 + 255 X^4 + 901 X^5 + 173 X^6 + 906 X^7 + 922 Y$ を得て、ベクトル $v_6=(397, 954, 514, 891, 922, 255, 0, 901, 0, 173, 0, 906)$ を生成する。

【 0 1 6 1 】

最後に、第七番目の単項式 $M_7=X Y$ に対して、 $X Y g = X Y (193 + 959 X + 364 X^2 + 180 X^3 + 550 Y + 43 X^4 + X^5)$ を $f=699 + 601 X + 688 X^2 + 281 X^3 + 217 Y + 287 X^4 + XY$ および $F=Y^2+X^7+7X$ で割ると、 $X Y g = (992 + 536 X + 805 X^2 + 906 X^3 + 195 X^4 + X^5 + 571 Y + 287 X Y) f + (200 + 258 X + 722 X^2) F + 784 + 420 X + 871 X^2 + 113 X^3 + 933 X^4 + 749 X^5 + 153 X^6 + 112 X^7 + 88 Y$ となるので、剰余 $784 + 420 X + 871 X^2 + 113 X^3 + 933 X^4 + 749 X^5 + 153 X^6 + 112 X^7 + 88 Y$ を得て、ベクトル $v_7=(784, 420, 871, 113, 88, 933, 0, 749, 0, 153, 0, 112)$ を生成する。以上で、第二のイデアル縮約部12の多項式ベクトル生成部32における処理を終了する。

次に、第二のイデアル縮約部12は、基底構成部33において、多項式ベクトル生成部32で生成した、7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を線形関係導出部34に入力し、出力として複数の7次元ベクトル m_1, m_2, \dots を得る。

【 0 1 6 2 】

線形関係導出部34は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術に属するので、以下、線形関係導出部34の動作はその概略のみ示す。線形関係導出部34は、まず、入力された7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を順に並べて 7×12 行列

【数 2 3】

$$M_R = \begin{pmatrix} 193 & 959 & 364 & 180 & 550 & 43 & 0 & 1 & 0 & 0 & 0 & 0 \\ 988 & 595 & 934 & 191 & 721 & 743 & 0 & 43 & 0 & 1 & 0 & 0 \\ 521 & 528 & 975 & 133 & 947 & 109 & 0 & 743 & 0 & 43 & 0 & 1 \\ 451 & 78 & 481 & 791 & 686 & 389 & 0 & 924 & 0 & 527 & 0 & 195 \\ 601 & 459 & 217 & 14 & 253 & 965 & 0 & 924 & 0 & 130 & 0 & 438 \\ 397 & 954 & 514 & 891 & 922 & 255 & 0 & 901 & 0 & 173 & 0 & 906 \\ 784 & 420 & 871 & 113 & 88 & 933 & 0 & 749 & 0 & 153 & 0 & 112 \end{pmatrix}$$

を構成する。

【 0 1 6 3 】

次に、線形関係導出部34は行列 M_R に7次元の単位行列を連結し、

【数 2 5】

$$\begin{pmatrix}
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 814 & 571 & 103 & 897 \\
 0 & 1 & 204 & 682 & 795 & 542 & 443 & 627 \\
 1 & 0 & 14 & 804 & 522 & 385 & 12 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 725 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 247 & 822 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 43 & 434 & 919 & 0 & 0 & 0 & 0 & 0 \\
 550 & 922 & 914 & 0 & 0 & 0 & 0 & 0 \\
 180 & 587 & 736 & 0 & 0 & 0 & 0 & 0 \\
 364 & 524 & 326 & 0 & 0 & 0 & 0 & 0 \\
 959 & 485 & 0 & 0 & 0 & 0 & 0 & 0 \\
 193 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{pmatrix}
 = E$$

よく知られているように行列 m の4から7行目の第13成分以降よりなるベクトルは、入力された7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ の全ての1次独立な線形従属関係 $\sum_{i=1}^7 m_{ji} v_i = 0$ ($j=1, 2, \dots, 7$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,7}), (m_{2,1}, m_{2,2}, \dots, m_{2,7}), \dots\}$ である。線形関係導出部34は、行列 m の4行目の第13成分以降よりなるベクトル $m_1=(804, 795, 814, 1, 0, 0, 0)$ 、行列 m の5行目の第13成分以降よりなるベクトル $m_2=(522, 542, 571, 0, 1, 0, 0)$ 、行列 m の6行目の第13成分以降よりなるベクトル $m_3=(385, 443, 103, 0, 0, 1, 0)$ および行列 m の7行目の第13成分以降よりなるベクトル $m_4=(12, 627, 897, 0, 0, 0, 1)$ を出

力する。

【 0 1 6 5 】

第一のイデアル縮約部12の基底構成部33における処理の説明に戻る。次に、この第二のイデアル縮約部12は、図11のグレブナ基底構成用テーブルを参照し前記値 $d=3$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(804, 795, 814, 1, 0, 0, 0)$,

$m_2=(522, 542, 571, 0, 1, 0, 0)$ 、

$m_3=(385, 443, 103, 0, 0, 1, 0)$ および

$m_4=(12, 627, 897, 0, 0, 0, 1)$

中に存在しないレコードを検索する。第11レコードの位数フィールドの値は3であり、第11レコードの成分番号リスト4,5,6,7に対応する成分がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第11レコードが得られる。

【 0 1 6 6 】

さらに第11レコードの第一ベクトル型の値は $(*, *, *, 1, 0, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(804, 795, 814, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, X^2, X^3, Y, X^4, XY の各単項式の係数の列とみなし、多項式 $f_1=804 + 795 X + 814 X^2 + X^3$ を生成する。

【 0 1 6 7 】

同様にして、第11レコードの第二ベクトル型の値は $(*, *, *, 0, 1, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(522, 542, 571, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, X^2, X^3, Y, X^4, XY の各単項式の係数の列とみなし、多項式 $f_2=522 + 542 X + 571 X^2 + Y$ を生成する。第11レコードの第三ベクトル型の値はnullなので、無視される。最後に、イデアル縮約装置12は、多項式の集合 $J^*=\{f_1, f_2\}=\{804 + 795 X + 814 X^2 + X^3, 522 + 542 X + 571 X^2 + Y\}$ を構成し、出力する。以上で、第一のイデアル縮約部12の動作は終了する。

【0 1 6 8】

次に、第二のイデアル縮約部13が、図3に示す機能ブロックの処理の流れにしたがって、図8の代数曲線パラメータファイルAおよび第一のイデアル縮約部12が出力したグレブナ基底 $J^* = \{f_1, f_2\} = \{804 + 795 X + 814 X^2 + X^3, 522 + 542 X + 571 X^2 + Y\}$ を入力として以下のように動作する。まず、イデアル縮約部13は、図3のイデアル型分類部31において、図9のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル J^* の型と一致するレコードを検索し第11レコードを得て、第11レコードのイデアル型番号フィールドの値 $N=31$ および縮約位数フィールドの値 $d=3$ を取得する。

【0 1 6 9】

次に、イデアル縮約部13は、前記 $d=3$ が0でないことを確認し、多項式ベクトル生成部32において、図10の単項式リストテーブルを参照し前記 $d=3$ を位数フィールドの値に持つレコードを検索し第4レコードを得て、第4レコードの単項式リストフィールドに記述されている単項式のリスト $1, X, X^2, X^3, Y, X^4, XY$ を取得する。さらに、イデアル縮約部13は、 J^* の第1要素 $f=804 + 795 X + 814 X^2 + X^3$ 、第2要素 $g=522 + 542 X + 571 X^2 + Y$ を取得し(J^* には第3要素はないので第3番目の多項式 h は用いない)、代数曲線パラメータファイルAの係数リスト $0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1$ を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, X^3, Y, X^4, XY, X^5, X^2 Y, X^6, X^3 Y, X^7, Y^2$ の各単項式の係数の列とみなして、定義多項式 $F=Y^2+X^7+7X$ を生成する。

【0 1 7 0】

次に、イデアル縮約部13は、前記単項式のリスト $1, X, X^2, X^3, Y, X^4, XY$ 中のそれぞれの M_i ($1 \leq i \leq 7$) に対して、 M_i と多項式 g の積 $M_i \cdot g$ の、多項式 f および F による剰余式 r_i を計算し、その係数を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, X^3, Y, X^4, XY, X^5, X^2 Y, X^6, X^3 Y, X^7$ の順にならべて、ベクトル v_i を生成する。すなわち、まず、第一番目の単項式 $M_1=1$ に対して、 $1 \cdot g = 522 + 542 X + 571 X^2 + Y$ を $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 522 + 542 X + 571 X^2 + Y$ となるので、剰余 $522 + 542 X + 571 X^2 + Y$ を得て、ベクトル $v_1=(522, 542, 571, 0, 1, 0, 0, 0, 0)$ を生成す

る。

【 0 1 7 1 】

次に、第二番目の単項式 $M_2=X$ に対して、 $X g = X (522 + 542 X + 571 X^2 + Y)$ を
 $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $X g = 571 f + 0 \cdot F$
 $+ 11 + 627 X + 897 X^2 + X Y$ となるので、剰余 $11 + 627 X + 897 X^2 + X Y$ を
 得て、ベクトル $v_2=(11, 627, 897, 0, 0, 0, 1, 0, 0)$ を生成する。

【 0 1 7 2 】

次に、第三番目の単項式 $M_3=X^2$ に対して、 $X^2 g = X^2 (522 + 542 X + 571 X^2 + Y)$
)を $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $X^2 g = (897 + 5$
 $71 X) f + 0 \cdot F + 247 + 259 X + 985 X^2 + X^2 Y$ となるので、剰余 $247 + 259 X$
 $+ 985 X^2 + X^2 Y$ を得て、ベクトル $v_3=(247, 259, 985, 0, 0, 0, 0, 0, 1)$ を生
 成する。

【 0 1 7 3 】

次に、第四番目の単項式 $M_4=X^3$ に対して、 $X^3 g = X^3 (522 + 542 X + 571 X^2 + Y)$
)を $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $X^3 g = (985 + 8$
 $97 X + 571 X^2 + Y) f + 0 \cdot F + 125 + 156 X + 624 X^2 + 205 Y + 214 X Y + 1$
 $95 X^2 Y$ となるので、剰余 $125 + 156 X + 624 X^2 + 205 Y + 214 X Y + 195 X^2 Y$
 を得て、ベクトル $v_4=(125, 156, 624, 0, 205, 0, 214, 0, 195)$ を生成する。

【 0 1 7 4 】

次に、第五番目の単項式 $M_5=Y$ に対して、 $Y g = Y (522 + 542 X + 571 X^2 + Y)$ を
 $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $Y g = (486 + 348 X$
 $+ 103 X^2 + 814 X^3 + 1008 X^4) f + 1 \cdot F + 748 + 780 X + 665 X^2 + 522 Y +$
 $542 X Y + 571 X^2 Y$ となるので、剰余 $748 + 780 X + 665 X^2 + 522 Y + 542 X Y$
 $+ 571 X^2 Y$ を得て、ベクトル $v_5=(748, 780, 665, 0, 522, 0, 542, 0, 571)$ を
 生成する。

【 0 1 7 5 】

次に、第六番目の単項式 $M_6=X^4$ に対して、 $X^4 g = X^4 (522 + 542 X + 571 X^2 + Y)$
)を $f=804 + 795 X + 814 X^2 + X^3$ および $F= Y^2+X^7+7X$ で割ると、 $X^4 g = (624 + 9$
 $85 X + 897 X^2 + 571 X^3 + 195 Y + X Y) f + 0 \cdot F + 786 + 473 X + 756 X^2 +$

624 Y + 566 X Y + 906 X² Yとなるので、剰余786 + 473 X + 756 X² + 624 Y + 566 X Y + 906 X² Yを得て、ベクトルv₆=(786, 473, 756, 0, 624, 0, 566, 0, 906)を生成する。

【 0 1 7 6 】

最後に、第七番目の単項式M₇=X Yに対して、X Y g = X Y (522 + 542 X + 571 X² + Y)をf=804 + 795 X + 814 X² + X³およびF= Y²+X⁷+7Xで割ると、X Y g = (665 + 486 X + 348 X² + 103 X³ + 814 X⁴ + 1008 X⁵ + 571 Y) f + X F + 110 + 789 X + 294 X² + 11 Y + 627 X Y + 897 X² Yとなるので、剰余110 + 789 X + 294 X² + 11 Y + 627 X Y + 897 X² Yを得て、ベクトルv₇=(110, 789, 294, 0, 11, 0, 627, 0, 897)を生成する。以上で、第二のイデアル縮約部13の多項式ベクトル生成部32における処理を終了する。

【 0 1 7 7 】

次に、このイデアル縮約装置13は、基底構成部33において、多項式ベクトル生成部32で生成した、7個の9次元ベクトルv₁, v₂, v₃, v₄, v₅, v₆, v₇を線形関係導出部34に入力し、出力として複数の7次元ベクトルm₁, m₂, ...を得る。線形関係導出部34は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術に属するので、以下、線形関係導出部34の動作はその概略のみ示す。

【 0 1 7 8 】

線形関係導出部34は、まず、入力された7個の9次元ベクトルv₁, v₂, v₃, v₄, v₅, v₆, v₇を順に並べて7x9行列

【数 2 6】

$$M_R = \begin{bmatrix} 522 & 542 & 571 & 0 & 1 & 0 & 0 & 0 & 0 \\ 11 & 627 & 897 & 0 & 0 & 0 & 1 & 0 & 0 \\ 247 & 259 & 985 & 0 & 0 & 0 & 0 & 0 & 1 \\ 125 & 156 & 624 & 0 & 205 & 0 & 214 & 0 & 195 \\ 748 & 780 & 665 & 0 & 522 & 0 & 542 & 0 & 571 \\ 786 & 473 & 756 & 0 & 624 & 0 & 566 & 0 & 906 \\ 110 & 789 & 294 & 0 & 11 & 0 & 627 & 0 & 897 \end{bmatrix}$$

を構成する。

【 0 1 7 9 】

次に、線形関係導出部34は、行列 M_R に7次元の単位行列を連結し、

【数 2 7】

$$M'_R = \begin{bmatrix} 522 & 542 & 571 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 11 & 627 & 897 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 247 & 259 & 985 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 125 & 156 & 624 & 0 & 205 & 0 & 214 & 0 & 195 & 0 & 0 & 0 & 1 & 0 & 0 \\ 748 & 780 & 665 & 0 & 522 & 0 & 542 & 0 & 571 & 0 & 0 & 0 & 0 & 1 & 0 \\ 786 & 473 & 756 & 0 & 624 & 0 & 566 & 0 & 906 & 0 & 0 & 0 & 0 & 0 & 1 \\ 110 & 789 & 294 & 0 & 11 & 0 & 627 & 0 & 897 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

を構成する。

【 0 1 8 0 】

次に、線形関係導出部34は、 i 行目の定数倍を $i+1$ 行目から7行目に加えることで($i=1, 2, 3$)、行列 M'_R を三角化し以下の行列 m を得る。

【数 2 8】

$$m = \begin{bmatrix} 522 & 542 & 571 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 171 & 48 & 0 & 230 & 0 & 1 & 0 & 0 & 230 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 976 & 0 & 385 & 0 & 53 & 0 & 1 & 385 & 53 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 804 & 795 & 814 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 487 & 467 & 438 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 385 & 443 & 103 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 998 & 382 & 112 & 0 & 0 & 1 \end{bmatrix}$$

【 0 1 8 1 】

よく知られているように行列 m の4から7行目の第10成分以降よりなるベクトルは、入力された7個の12次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ の全ての1次独立な線形従属関係 $\sum_{i=1}^7 m_{ji} v_i = 0$ ($j=1, 2, \dots$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,n}), (m_{2,1}, m_{2,2}, \dots, m_{2,n}), \dots\}$ である。線形関係導出部34は、行列 m の4行目の第10成分以降よりなるベクトル $m_1 = (804, 795, 814, 1, 0, 0, 0)$ 、行列 m の5行目の第10成分以降よりなるベクトル $m_2 = (487, 467, 438, 0, 1, 0, 0)$ 、行列 m の6行目の

第10成分以降よりなるベクトル $m_3=(385, 443, 103, 0, 0, 1, 0)$ および行列 m の7行目の第10成分以降よりなるベクトル $m_4=(998, 382, 112, 0, 0, 0, 1)$ を出力する。

【 0 1 8 2 】

第二のイデアル縮約部13の基底構成部33における処理の説明に戻る。次に、このイデアル縮約部13は、図11のグレブナ基底構成用テーブルを参照し前記値 $d=3$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(804, 795, 814, 1, 0, 0, 0)$ 、 $m_2=(487, 467, 438, 0, 1, 0, 0)$ 、 $m_3=(385, 443, 103, 0, 0, 1, 0)$ および $m_4=(998, 382, 112, 0, 0, 0, 1)$ 中に存在しないレコードを検索する。第11レコードの位数フィールドの値は3であり、第11レコードの成分番号リスト4,5,6,7がすべて0であるベクトルは m_1, m_2, m_3, m_4 には存在していないので、検索結果として第11レコードが得られる。

【 0 1 8 3 】

さらに第11レコードの第一ベクトル型の値は $(*, *, *, 1, 0, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(804, 795, 814, 1, 0, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, X^2, X^3, Y, X^4, XY の各単項式の係数の列とみなし、多項式 $f_1=804 + 795 X + 814 X^2 + X^3$ を生成する。

【 0 1 8 4 】

同様にして、第11レコードの第二ベクトル型の値は $(*, *, *, 0, 1, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(487, 467, 438, 0, 1, 0, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, X^2, X^3, Y, X^4, XY の各単項式の係数の列とみなし、多項式 $f_2=487 + 467 X + 438 X^2 + Y$ を生成する。第11レコードの第三ベクトル型の値はnullなので、無視される。

【 0 1 8 5 】

最後に、イデアル縮約部13は、多項式の集合 $J^{**}=\{f_1, f_2\}=\{804 + 795 X + 814 X^2 + X^3, 487 + 467 X + 438 X^2 + Y\}$ を構成し、出力する。以上で、第二のイデ

アル縮約部13の動作は終了する。最後に、図1のヤコビ群加算装置において、イデアル縮約部13の出力したグレブナ基底 $J^{**} = \{804 + 795 X + 814 X^2 + X^3, 487 + 467 X + 438 X^2 + Y\}$ が出力装置より出力される。

次に、C₂₅曲線を用いた場合の実施例を示す。本実施例では、代数曲線パラメータファイルとして図12の代数曲線パラメータファイルを、イデアル型テーブルとして図13のイデアル型テーブルを、単項式リストテーブルとして図14の単項式リストテーブルを、グレブナ基底構成用テーブルとして図15のグレブナ基底構成用テーブルを用いる。

【 0 1 8 6 】

図1のヤコビ群要素加算装置において、図12の代数曲線パラメータファイルAおよび代数曲線パラメータファイルAで指定されたC₂₅曲線のヤコビ群の要素を表す、代数曲線パラメータファイルAで指定された代数曲線の座標環のイデアルのグレブナ基底

$$I_1 = \{729 + 88 X + X^2, 475 + 124 X + Y\}$$

および

$$I_2 = \{180 + 422 X + X^2, 989 + 423 X + Y\}$$

が入力されたとする。

【 0 1 8 7 】

まず、イデアル合成部11が、図2に示す機能ブロックの処理の流れにしたがって、図12の代数曲線パラメータファイルA、上記グレブナ基底 I_1 および I_2 を入力として以下のように動作する。イデアル合成部11は、まず、図2のイデアル型分類部21において、図13のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル I_1 の型と一致するレコードを検索し第6レコードを得て、第6レコードのイデアル型番号フィールドの値 $N_1=21$ および位数フィールドの値 $d_1=2$ を取得する。同様に、イデアル型が入力イデアル I_2 の型と一致するレコードを検索し第6レコードを得て、第6レコードのイデアル型番号フィールドの値 $N_2=21$ および位数フィールドの値 $d_2=2$ を取得する。

【 0 1 8 8 】

次に、イデアル合成部11は、単項式ベクトル生成部22において、前記位数フィー

ルドの値 $d_1=2$ および $d_2=2$ の和 $d_3=d_1+d_2=4$ を計算し、図14の単項式リストテーブルを参照し前記 $d_3=4$ を位数フィールドの値に持つレコードを検索し第1レコードを得て、第1レコードの単項式リストフィールドに記述されている単項式のリスト1, X , X^2 , Y , X^3 , XY , X^4 を取得する。 I_1 と I_2 は異なるので、前記単項式のリスト1, X , X^2 , Y , X^3 , XY , X^4 中のそれぞれの M_i ($1 \leq i \leq 7$)に対して、 M_i を I_1 で割った剰余を計算し、多項式 $a^{(i)}_1 + a^{(i)}_2 X$ を得て、その係数を、代数曲線パラメータファイルAの単項式順序1, X , \dots の順にならべて、ベクトル $w^{(i)}_1 = (a^{(i)}_1, a^{(i)}_2)$ を生成する。

【 0 1 8 9 】

さらに、 M_i を I_2 で割った剰余を計算し、多項式 $b^{(i)}_1 + b^{(i)}_2 X$ を得て、その係数を、代数曲線パラメータファイルAの単項式順序1, X , \dots の順にならべて、ベクトル $w^{(i)}_2 = (b^{(i)}_1, b^{(i)}_2)$ を生成し、上記2つのベクトル $w^{(i)}_1$ と $w^{(i)}_2$ を連結してベクトル $v_i = (a^{(i)}_1, a^{(i)}_2, b^{(i)}_1, b^{(i)}_2)$ を生成する。すなわち、 $M_1 = 1$ を I_1 でわると、 $1 = 0 \cdot (729 + 88 X + X^2) + 0 \cdot (475 + 124 X + Y) + 1$ となるので、剰余として1を得て、ベクトル $w^{(1)}_1 = (1, 0)$ を生成する。さらに、 $M_1 = 1$ を I_2 でわると、 $1 = 0 \cdot (180 + 422 X + X^2) + 0 \cdot (989 + 423 X + Y) + 1$ となるので、剰余として1を得て、ベクトル $w^{(1)}_2 = (1, 0)$ を生成する。 $w^{(1)}_1$ と $w^{(1)}_2$ を連結して、ベクトル $v_1 = (1, 0, 1, 0)$ を生成する。

【 0 1 9 0 】

次に、 $M_2 = X$ を I_1 でわると、 $X = 0 \cdot (729 + 88 X + X^2) + 0 \cdot (475 + 124 X + Y) + X$ となるので、剰余として X を得て、ベクトル $w^{(2)}_1 = (0, 1)$ を生成する。さらに、 $M_2 = X$ を I_2 でわると、 $X = 0 \cdot (180 + 422 X + X^2) + 0 \cdot (989 + 423 X + Y) + X$ となるので、剰余として X を得て、ベクトル $w^{(2)}_2 = (0, 1)$ を生成する。 $w^{(2)}_1$ と $w^{(2)}_2$ を連結して、ベクトル $v_2 = (0, 1, 0, 1)$ を生成する。

【 0 1 9 1 】

次に、 $M_3 = X^2$ を I_1 でわると、 $X^2 = 1 \cdot (729 + 88 X + X^2) + 0 \cdot (475 + 124 X + Y) + 280 + 921 X$ となるので、剰余として $280 + 921 X$ を得て、ベクトル $w^{(3)}_1 = (280, 921)$ を生成する。さらに、 $M_3 = X^2$ を I_2 でわると、 $X^2 = 1 \cdot (180 + 422 X + X^2) + 0 \cdot (989 + 423 X + Y) + 829 + 587 X$ となるので、剰余として 829

+ 587 X を得て、ベクトル $w^{(3)}_2 = (829, 587)$ を生成する。 $w^{(3)}_1$ と $w^{(3)}_2$ を連結して、ベクトル $v_3 = (280, 921, 829, 587)$ を生成する。

【 0 1 9 2 】

次に、 $M_4 = Y$ を I_1 でわると、 $Y = 0 \cdot (729 + 88 X + X^2) + 1 \cdot (475 + 124 X + Y) + 534 + 885 X$ となるので、剰余として $534 + 885 X$ を得て、ベクトル $w^{(4)}_1 = (534, 885)$ を生成する。さらに、 $M_4 = Y$ を I_2 でわると、 $Y = 0 \cdot (180 + 422 X + X^2) + 1 \cdot (989 + 423 X + Y) + 20 + 586 X$ となるので、剰余として $20 + 586 X$ を得て、ベクトル $w^{(4)}_2 = (20, 586)$ を生成する。 $w^{(4)}_1$ と $w^{(4)}_2$ を連結して、ベクトル $v_4 = (534, 885, 20, 586)$ を生成する。

【 0 1 9 3 】

次に、 $M_5 = X^3$ を I_1 でわると、 $X^3 = (921 + X)(729 + 88 X + X^2) + 0 \cdot (475 + 124 X + Y) + 585 + 961 X$ となるので、剰余として $585 + 961 X$ を得て、ベクトル $w^{(5)}_1 = (585, 961)$ を生成する。

【 0 1 9 4 】

さらに、 $M_5 = X^3$ を I_2 でわると、 $X^3 = (587 + X)(180 + 422 X + X^2) + 0 \cdot (989 + 423 X + Y) + 285 + 320 X$ となるので、剰余として $285 + 320 X$ を得て、ベクトル $w^{(5)}_2 = (285, 320)$ を生成する。 $w^{(5)}_1$ と $w^{(5)}_2$ を連結して、ベクトル $v_5 = (585, 961, 285, 320)$ を生成する。次に、 $M_6 = XY$ を I_1 でわると、 $XY = 885(729 + 88 X + X^2) + X(475 + 124 X + Y) + 595 + 347 X$ となるので、剰余として $595 + 347 X$ を得て、ベクトル $w^{(6)}_1 = (595, 347)$ を生成する。

【 0 1 9 5 】

さらに、 $M_6 = XY$ を I_2 でわると、 $XY = 586(180 + 422 X + X^2) + X(989 + 423 X + Y) + 465 + 942 X$ となるので、剰余として $465 + 942 X$ を得て、ベクトル $w^{(6)}_2 = (465, 942)$ を生成する。 $w^{(6)}_1$ と $w^{(6)}_2$ を連結して、ベクトル $v_6 = (595, 347, 465, 942)$ を生成する。

【 0 1 9 6 】

最後に、 $M_7 = X^4$ を I_1 でわると、 $X^4 = (961 + 921 X + X^2)(729 + 88 X + X^2) + 0 \cdot (475 + 124 X + Y) + 686 + 773 X$ となるので、剰余として $686 + 773 X$ を得て、ベクトル $w^{(7)}_1 = (686, 773)$ を生成する。さらに、 $M_7 = X^4$ を I_2 でわると、

$X^4 = (320 + 587 X + X^2) (180 + 422 X + X^2) + 0 \cdot (989 + 423 X + Y) + 922 + 451 X$ となるので、剰余として $922 + 451 X$ を得て、ベクトル $w^{(7)}_2 = (922, 451)$ を生成する。 $w^{(7)}_1$ と $w^{(7)}_2$ を連結して、ベクトル $v_7 = (686, 773, 922, 451)$ を生成する。以上で、イデアル合成装置11の、単項式ベクトル生成部22における処理を終了する。

【 0 1 9 7 】

次に、イデアル合成部11は、基底構成部23において、単項式ベクトル生成部22で生成した、7個の4次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を線形関係導出装置24に入力し、出力として複数の7次元ベクトル m_1, m_2, \dots を得る。線形関係導出部24は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術であるので、以下、線形関係導出部24の動作はその概略のみ示す。線形関係導出部24は、まず、入力された7個の4次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ を順に並べて 7×4 行列

【数 2 9】

$$M_c = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 280 & 921 & 829 & 587 \\ 534 & 885 & 20 & 586 \\ 585 & 961 & 285 & 320 \\ 595 & 347 & 465 & 942 \\ 686 & 773 & 922 & 451 \end{pmatrix}$$

を構成する。

【 0 1 9 8 】

次に、線形関係導出部24は、行列 M_c に7次元の単位行列を連結し、

【数 3 0】

$$M'_C = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 280 & 921 & 829 & 587 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 534 & 885 & 20 & 586 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 585 & 961 & 285 & 320 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 595 & 347 & 465 & 942 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 686 & 773 & 922 & 451 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

を得る。

【0 1 9 9】

次に、線形関係導出部24は、 i 行目の定数倍を $i+1$ 行目から7行目に加えることで($i=1, 2, \dots, 4$)、行列 M'_C を三角化し、以下の行列 m を得る。

【数 3 1】

$$m = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 549 & 675 & 729 & 88 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 548 & 744 & 789 & 363 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 444 & 709 & 900 & 42 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 969 & 716 & 940 & 619 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 635 & 230 & 807 & 778 & 0 & 0 & 1 \end{pmatrix}$$

【0 2 0 0】

よく知られているように行列 m の5から7行目の第5成分以降よりなるベクトルは、入力された7個の4次元ベクトル $v_1, v_2, v_3, v_4, v_5, v_6, v_7$ の全ての1次独立な線形従属関係 $\sum_{i=1}^7 m_{ji} v_i = 0$ ($j=1, 2, \dots, 7$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,7}), (m_{2,1}, m_{2,2}, \dots, m_{2,7}), \dots\}$ である。

【0 2 0 1】

線形関係導出部24は、行列 m の5行目の第5成分以降よりなるベクトル $m_1=(444, 709, 900, 42, 1, 0, 0)$ 、行列 m の6行目の第5成分以降よりなるベクトル $m_2=(969, 716, 940, 619, 0, 1, 0)$ および行列 m の7行目の第5成分以降よりなるベクトル m_3

$= (635, 230, 807, 778, 0, 0, 1)$ を出力する。

【 0 2 0 2 】

イデアル合成部11の基底構成部23における処理の説明に戻る。次に、イデアル合成部11は、図15のグレブナ基底構成用テーブルを参照し前記値 $d_3=4$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1=(444, 709, 900, 42, 1, 0, 0)$ 、 $m_2=(969, 716, 940, 619, 0, 1, 0)$ および $m_3=(635, 230, 807, 778, 0, 0, 1)$ 中に存在しないレコードを検索する。第1レコードの位数フィールドの値は4であり、第1レコードの成分番号リスト5,6,7に対応する成分がすべて0であるベクトルは m_1, m_2, m_3 には存在していないので、検索結果として第1レコードが得られる。

【 0 2 0 3 】

さらに第1レコードの第一ベクトル型の値は $(*, *, *, *, 1, 0, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1=(444, 709, 900, 42, 1, 0, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , Y, X^3 , XY, X^4 の各単項式の係数の列とみなし、多項式 $f_1=444 + 709 X + 900 X^2 + 42 Y + X^3$ を生成する。

【 0 2 0 4 】

同様にして、第1レコードの第二ベクトル型の値は $(*, *, *, *, 0, 1, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2=(969, 716, 940, 619, 0, 1, 0)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , Y, X^3 , XY, X^4 の各単項式の係数の列とみなし、多項式 $f_2=969 + 716 X + 940 X^2 + 619 Y + X Y$ を生成する。第1レコードの第三ベクトル型の値はnullなので、無視される。最後に、イデアル合成部11は、多項式の集合 $J=\{f_1, f_2\}=\{444 + 709 X + 900 X^2 + 42 Y + X^3, 969 + 716 X + 940 X^2 + 619 Y + X Y\}$ を構成し、出力する。以上で、イデアル合成部11の動作は終了する。

【 0 2 0 5 】

次に、第一のイデアル縮約部12が、図3に示す機能ブロックの処理の流れにしたがって、図12の代数曲線パラメータファイルAおよびイデアル合成部11が出力し

たグレブナ基底 $J = \{444 + 709 X + 900 X^2 + 42 Y + X^3, 969 + 716 X + 940 X^2 + 619 Y + X Y\}$ を入力として以下のように動作する。まず、第一のイデアル縮約部12は、図3のイデアル型分類部31において、図12のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアルJの型と一致するレコードを検索し第1レコードを得て、第1レコードのイデアル型番号フィールドの値 $N=41$ および縮約位数フィールドの値 $d=2$ を取得する。

【 0 2 0 6 】

次に、イデアル縮約部12は、前記 $d=2$ が0でないことを確認し、多項式ベクトル生成部32において、図14の単項式リストテーブルを参照し前記 $d=2$ を位数フィールドの値に持つレコードを検索し第3レコードを得て、第3レコードの単項式リストフィールドに記述されている単項式のリスト $1, X, X^2, Y$ を取得する。さらに、イデアル縮約部12は、Jの第1要素 $f=444 + 709 X + 900 X^2 + 42 Y + X^3$ 、第2要素 $g=969 + 716 X + 940 X^2 + 619 Y + X Y$ を取得し(Jには第3要素はないので第3番目の多項式hは用いない)、代数曲線パラメータファイルAの係数リスト $0, 7, 0, 0, 0, 0, 0, 1, 1$ を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, Y, X^3, XY, X^4, X^2 Y, X^5, Y^2$ の各単項式の係数の列とみなして、定義多項式 $F=Y^2+X^5+7X$ を生成する。

【 0 2 0 7 】

次に、イデアル縮約部12は、前記単項式のリスト $1, X, X^2, Y$ 中のそれぞれの M_i ($1 \leq i \leq 4$) に対して、 M_i と多項式 g の積 $M_i \cdot g$ の、多項式 f および F による剰余式 r_i を計算し、その係数を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, Y, X^3, XY, X^4, X^2 Y$ の順にならべて、ベクトル v_i を生成する。すなわち、まず、第一番目の単項式 $M_1=1$ に対して、 $1 \cdot g = 969 + 716 X + 940 X^2 + 619 Y + X Y$ を $f=444 + 709 X + 900 X^2 + 42 Y + X^3$ および $F=Y^2+X^5+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 969 + 716 X + 940 X^2 + 619 Y + X Y$ となるので、剰余 $969 + 716 X + 940 X^2 + 619 Y + X Y$ を得て、ベクトル $v_1=(969, 716, 940, 619, 0, 1, 0, 0)$ を生成する。

【 0 2 0 8 】

次に、第二番目の単項式 $M_2=X$ に対して、 $X \cdot g = X (969 + 716 X + 940 X^2 + 619$

$Y + X Y)$ を $f=444 + 709 X + 900 X^2 + 42 Y + X^3$ および $F= Y^2+X^5+7X$ で割ると、
 $X g = 940 f + 0 \cdot F + 366 + 449 X + 258 X^2 + 880 Y + 619 X Y + X^2 Y$ となる
 ので、剰余 $366 + 449 X + 258 X^2 + 880 Y + 619 X Y + X^2 Y$ を得て、ベクトル $v_2=(366, 449, 258, 880, 0, 619, 0, 1)$ を生成する。

次に、第三番目の単項式 $M_3=X^2$ に対して、 $X^2 g = X^2 (969 + 716 X + 940 X^2 + 619 Y + X Y)$ を $f=444 + 709 X + 900 X^2 + 42 Y + X^3$ および $F= Y^2+X^5+7X$ で割ると、
 $X^2 g = (297 + 473 X + 42 X^2 + Y) f + 967 F + 311 + 462 X + 199 X^2 + 199 Y + 614 X Y + 982 X^2 Y$ となるので、剰余 $311 + 462 X + 199 X^2 + 199 Y + 614 X Y + 982 X^2 Y$ を得てベクトル $v_3=(311, 462, 199, 199, 0, 614, 0, 982)$ を生成する。

【 0 2 0 9 】

最後に、第四番目の単項式 $M_4=Y$ に対して、 $Y g = Y (969 + 716 X + 940 X^2 + 619 Y + X Y)$ を $f=444 + 709 X + 900 X^2 + 42 Y + X^3$ および $F= Y^2+X^5+7X$ で割ると、
 $Y g = (994 + 625 X + 27 X^2 + 1008 X^3 + 42 Y) f + (873 + X) F + 606 + 463 X + 322 X^2 + 104 Y + 183 X Y + 348 X^2 Y$ となるので、剰余 $606 + 463 X + 322 X^2 + 104 Y + 183 X Y + 348 X^2 Y$ を得て、ベクトル $v_4=(606, 463, 322, 104, 0, 183, 0, 348)$ を生成する。以上で、イデアル縮約装置12の、多項式ベクトル生成部32における処理を終了する。

次に、第一のイデアル縮約部12は、基底構成部33において、多項式ベクトル生成部32で生成した、4個の8次元ベクトル v_1, v_2, v_3, v_4 を線形関係導出部34に入力し、出力として複数の4次元ベクトル m_1, m_2, \dots を得る。線形関係導出部34は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術に属するので、以下、線形関係導出部34の動作はその概略のみ示す。

【 0 2 1 0 】

線形関係導出部34は、まず、入力された4個の8次元ベクトル v_1, v_2, v_3, v_4 を順に並べて 4×8 行列

【数 3 2】

$$M_R = \begin{bmatrix} 969 & 716 & 940 & 619 & 0 & 1 & 0 & 0 \\ 366 & 449 & 258 & 880 & 0 & 619 & 0 & 1 \\ 311 & 462 & 199 & 199 & 0 & 614 & 0 & 982 \\ 606 & 463 & 322 & 104 & 0 & 183 & 0 & 348 \end{bmatrix}$$

を構成する。

【 0 2 1 1】

次に、線形関係導出部34は、行列 M_R に4次元の単位行列を連結し、

【数 3 3】

$$M'_R = \begin{bmatrix} 969 & 716 & 940 & 619 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 366 & 449 & 258 & 880 & 0 & 619 & 0 & 1 & 0 & 1 & 0 & 0 \\ 311 & 462 & 199 & 199 & 0 & 614 & 0 & 982 & 0 & 0 & 1 & 0 \\ 606 & 463 & 322 & 104 & 0 & 183 & 0 & 348 & 0 & 0 & 0 & 1 \end{bmatrix}$$

を構成する。

【 0 2 1 2】

次に、線形関係導出部34は、 i 行目の定数倍を $i+1$ 行目から4行目に加えることで($i=1, 2$)、行列 M'_R を三角化し以下の行列 m を得る。

【数 3 4】

$$m = \begin{bmatrix} 969 & 716 & 940 & 619 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 341 & 787 & 848 & 0 & 275 & 0 & 1 & 665 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 835 & 27 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 312 & 661 & 0 & 1 \end{bmatrix}$$

【 0 2 1 3】

よく知られているように行列 m の3から4行目の第9成分以降よりなるベクトルは、
 入力された4個の8次元ベクトル v_1, v_2, v_3, v_4 の全ての1次独立な線形従属関係 $\sum_{i=1}^4 m_{ji} v_i = 0$ ($j=1, 2, \dots$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,4}), (m_{2,1}, m_{2,2},$

, ..., $m_2, 4$), ...} である。線形関係導出部34は、行列 m の3行目の第9成分以降よりなるベクトル $m_1 = (835, 27, 1, 0)$ および行列 m の4行目の第9成分以降よりなるベクトル $m_2 = (312, 661, 0, 1)$ を出力する。

【 0 2 1 4 】

第一のイデアル縮約部12の基底構成部33における処理の説明に戻る。次に、イデアル縮約部12は、図15のグレブナ基底構成用テーブルを参照し前記値 $d=2$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベクトル $m_1 = (835, 27, 1, 0)$ および $m_2 = (312, 661, 0, 1)$ 中に存在しないレコードを検索する。第6レコードの位数フィールドの値は2であり、第6レコードの成分番号リスト3,4に対応する成分がすべて0であるベクトルは m_1, m_2 には存在していないので、検索結果として第6レコードが得られる。

【 0 2 1 5 】

さらに第6レコードの第一ベクトル型の値は $(*, *, 1, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1 = (835, 27, 1, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X , X^2 , Y の各単項式の係数の列とみなし、多項式 $f_1 = 835 + 27 X + X^2$ を生成する。同様にして、第6レコードの第二ベクトル型の値は $(*, *, 0, 1)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2 = (312, 661, 0, 1)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X , X^2 , Y の各単項式の係数の列とみなし、多項式 $f_2 = 312 + 661 X + Y$ を生成する。第6レコードの第三ベクトル型の値はnullなので、無視される。最後に、イデアル縮約装置12は、多項式の集合 $J^* = \{f_1, f_2\} = \{835 + 27 X + X^2, 312 + 661 X + Y\}$ を構成し、出力する。以上で、第一のイデアル縮約部12の動作は終了する。

【 0 2 1 6 】

次に、第二のイデアル縮約部13が、図3に示す機能ブロックの処理の流れにしたがって、図12の代数曲線パラメータファイルAおよび第一のイデアル縮約部12が出力したグレブナ基底 $J^* = \{f_1, f_2\} = \{835 + 27 X + X^2, 312 + 661 X + Y\}$ を入力として以下のように動作する。まず、第二のイデアル縮約部13は、図3のイデア

ル型分類部31において、図13のイデアル型テーブルを参照し、イデアル型フィールドに記述されているイデアル型が入力イデアル J^* の型と一致するレコードを検索し第6レコードを得て、第6レコードのイデアル型番号フィールドの値 $N=21$ および縮約位数フィールドの値 $d=2$ を取得する。

【 0 2 1 7 】

次に、イデアル縮約部13は、前記 $d=2$ が0でないことを確認し、多項式ベクトル生成部32において、図14の単項式リストテーブルを参照し前記 $d=2$ を位数フィールドの値に持つレコードを検索し第3レコードを得て、第3レコードの単項式リストフィールドに記述されている単項式のリスト $1, X, X^2, Y$ を取得する。さらに、イデアル縮約部13は、 J^* の第1要素 $f=835 + 27 X + X^2$ および第2要素 $g=312 + 661 X + Y$ を取得し(J^* には第3要素はないので第3番目の多項式 h は用いない)、代数曲線パラメータファイルAの係数リスト $0, 7, 0, 0, 0, 0, 0, 0, 1, 1$ を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, Y, X^3, XY, X^4, X^2 Y, X^5, Y^2$ の各単項式の係数の列とみなして、定義多項式 $F=Y^2+X^5+7X$ を生成する。

【 0 2 1 8 】

次に、イデアル縮約部13は、前記単項式のリスト $1, X, X^2, Y$ のそれぞれの M_i ($1 \leq i \leq 4$)に対して、 M_i と多項式 g の積 $M_i g$ の、多項式 f および F による剰余式 r_i を計算し、その係数を、代数曲線パラメータファイルAの単項式順序 $1, X, X^2, Y, X^3, XY, X^4, X^2 Y$ の順にならべて、ベクトル v_i を生成する。すなわち、まず、第一番目の単項式 $M_1=1$ に対して、 $1 \cdot g = 312 + 661 X + Y$ を $f=835 + 27 X + X^2$ および $F= Y^2+X^5+7X$ で割ると、 $g = 0 \cdot f + 0 \cdot F + 312 + 661 X + Y$ となるので、剰余 $312 + 661 X + Y$ を得て、ベクトル $v_1=(312, 661, 0, 1, 0, 0)$ を生成する。

【 0 2 1 9 】

次に、第二番目の単項式 $M_2=X$ に対して、 $X g = X (312 + 661 X + Y)$ を $f=835 + 27 X + X^2$ および $F= Y^2+X^5+7X$ で割ると、 $X g = 661 f + 0 \cdot F + 997 + 627 X + X Y$ となるので、剰余 $997 + 627 X + X Y$ を得て、ベクトル $v_2=(997, 627, 0, 0, 0, 1)$ を生成する。次に、第三番目の単項式 $M_3=X^2$ に対して、 $X^2 g = X^2 (312 + 661 X + Y)$ を $f=835 + 27 X + X^2$ および $F= Y^2+X^5+7X$ で割ると、 $X^2 g = (627 + 661 X + Y) f + 0 \cdot F + 126 + 212 X + 174 Y + 982 X Y$ となるので、剰余 $126 + 212$

$X + 174 \cdot Y + 982 \cdot X \cdot Y$ を得て、ベクトル $v_3=(126, 212, 0, 174, 0, 982)$ を生成する。

【 0 2 2 0 】

最後に、第四番目の単項式 $M_4=Y$ に対して、 $Y \cdot g = Y (312 + 661 X + Y)$ を $f=835 + 27 X + X^2$ および $F= Y^2+X^5+7X$ で割ると、 $Y \cdot g = (827 + 106 X + 27 X^2 + 1008 X^3) \cdot f + 1 \cdot F + 620 + 144 X + 312 Y + 661 X \cdot Y$ となるので、剰余 $620 + 144 X + 312 Y + 661 X \cdot Y$ を得て、ベクトル $v_4=(620, 144, 0, 312, 0, 661)$ を生成する。以上で、第二のイデアル縮約部13の多項式ベクトル生成部32における処理を終了する。

【 0 2 2 1 】

次に、この第二のイデアル縮約部13は、基底構成部33において、多項式ベクトル生成部32で生成した、4個の6次元ベクトル v_1, v_2, v_3, v_4 を線形関係導出部34に入力し、出力として複数の4次元ベクトル m_1, m_2, \dots を得る。線形関係導出部34は、掃き出し法を用いて、入力されたベクトルの線形関係を導出する。掃き出し法は既知の技術に属するので、以下、線形関係導出部34の動作はその概略のみ示す。

【 0 2 2 2 】

線形関係導出部34は、まず、入力された4個の6次元ベクトル v_1, v_2, v_3, v_4 を順に並べて4x6行列

【数 3 5】

$$M_R = \begin{bmatrix} 312 & 661 & 0 & 1 & 0 & 0 \\ 997 & 627 & 0 & 0 & 0 & 1 \\ 126 & 212 & 0 & 174 & 0 & 982 \\ 620 & 144 & 0 & 312 & 0 & 661 \end{bmatrix}$$

を構成する。

【 0 2 2 3 】

次に、線形関係導出部34は、行列 M_R に4次元の単位行列を連結し、

【数 3 6】

$$M'_R = \begin{bmatrix} 312 & 661 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 997 & 627 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 126 & 212 & 0 & 174 & 0 & 982 & 0 & 0 & 1 & 0 \\ 620 & 144 & 0 & 312 & 0 & 661 & 0 & 0 & 0 & 1 \end{bmatrix}$$

を構成する。

【 0 2 2 4 】

次に、線形関係導出部34は、 i 行目の定数倍を $i+1$ 行目から4行目に加えることで($i=1, 2$)、行列 M'_R を三角化し以下の行列 m を得る。

【数 3 7】

$$m = \begin{bmatrix} 312 & 661 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 536 & 0 & 815 & 0 & 1 & 815 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 835 & 27 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 697 & 348 & 0 & 1 \end{bmatrix}$$

【 0 2 2 5 】

よく知られているように行列 m の3から4行目の第7成分以降よりなるベクトルは、入力された4個の6次元ベクトル v_1, v_2, v_3, v_4 の全ての1次独立な線形従属関係 $\sum_{i=1}^4 m_{ji} v_i = 0$ ($j=1, 2, \dots$)を表すベクトル $\{(m_{1,1}, m_{1,2}, \dots, m_{1,4}), (m_{2,1}, m_{2,2}, \dots, m_{2,4}), \dots\}$ である。

【 0 2 2 6 】

線形関係導出部34は、行列 m の3行目の第7成分以降よりなるベクトル $m_1 = (835, 27, 1, 0)$ および、行列 m の4行目の第7成分以降よりなるベクトル $m_2 = (697, 348, 0, 1)$ を出力する。イデアル縮約部13の基底構成部33における処理の説明に戻る。
次に、イデアル縮約部13は、図15のグレブナ基底構成用テーブルを参照し前記値 $d=2$ を位数フィールドの値にもち、かつ成分番号リストフィールドに記述されているすべての成分番号に対応する成分がすべて0であるベクトルが前記複数のベ

クトル $m_1 = (835, 27, 1, 0)$ および $m_2 = (697, 348, 0, 1)$ 中に存在しないレコードを検索する。第6レコードの位数フィールドの値は2であり、第6レコードの成分番号リスト3,4がすべて0であるベクトルは m_1, m_2 には存在していないので、検索結果として第6レコードが得られる。

【0 2 2 7】

さらに、第6レコードの第一ベクトル型の値は $(*, *, 1, 0)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_1 = (835, 27, 1, 0)$ と合致するので、ベクトル m_1 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , Yの各単項式の係数の列とみなし、多項式 $f_1 = 835 + 27 X + X^2$ を生成する。同様にして、第6レコードの第二ベクトル型の値は $(*, *, 0, 1)$ であり(記号*はすべての数を表すと解釈する)、これはベクトル $m_2 = (697, 348, 0, 1)$ と合致するので、ベクトル m_2 を、代数曲線パラメータファイルAの単項式順序1, X, X^2 , Yの各単項式の係数の列とみなし、多項式 $f_2 = 697 + 348 X + Y$ を生成する。第6レコードの第三ベクトル型の値はnullなので、無視される。最後に、イデアル縮約部13は、多項式の集合 $J^{**} = \{f_1, f_2\} = \{835 + 27 X + X^2, 697 + 348 X + Y\}$ を構成し、出力する。以上で、イデアル縮約部13の動作は終了する。

【0 2 2 8】

最後に、図1のヤコビ群加算装置において、第二のイデアル縮約部13の出力したグレブナ基底 $J^{**} = \{835 + 27 X + X^2, 697 + 348 X + Y\}$ が出力装置より出力される。

【0 2 2 9】

【発明の効果】

本発明を用いることにより、 C_{ab} 曲線のヤコビ群における加算を高速に計算することができ、 C_{ab} 曲線の実用性を向上させることができるという効果がある。

【図面の簡単な説明】

【図 1】

本発明の実施の形態を示すブロック図である。

【図 2】

イデアル合成部の機能ブロック図である。

【図 3】

イデアル縮約部の機能ブロック図である。

【図 4】

C_{34} 曲線に対する代数曲線パラメータファイル A の一具体例である。

【図 5】

C_{34} 曲線に対するイデアル型テーブルの一具体例である。

【図 6】

C_{34} 曲線に対する単項式リストテーブルの一具体例である。

【図 7】

C_{34} 曲線に対するグレブナ基底構成用テーブルの一具体例である。

【図 8】

C_{27} 曲線に対する代数曲線パラメータファイルの一具体例である。

【図 9】

C_{27} 曲線に対するイデアル型テーブルの一具体例である。

【図 1 0】

C_{27} 曲線に対する単項式リストテーブルの一具体例である。

【図 1 1】

C_{27} 曲線に対するグレブナ基底構成用テーブルの一具体例である。

【図 1 2】

C_{25} 曲線に対する代数曲線パラメータファイルの一具体例である。

【図 1 3】

C_{25} 曲線に対するイデアル型テーブルの一具体例である。

【図 1 4】

C_{25} 曲線に対する単項式リストテーブルの一具体例である。

【図 1 5】

C_{25} 曲線に対するグレブナ基底構成用テーブルの一具体例である。

【図 1 6】

本発明によるヤコビ群加算アルゴリズムの演算量を示す図表である。

【符号の説明】

1.0; 2.0; 3 0 代数曲線パラメータファイル A

1 1 イdeal合成部

1 2 第一のイdeal縮約部

1 3 第二のイdeal縮約部

2 1, 3 1 イdeal型分類部

2 2 単項式ベクトル生成部

2 3, 3 3 基底構成部

2 4, 3 4 線形関係導出部

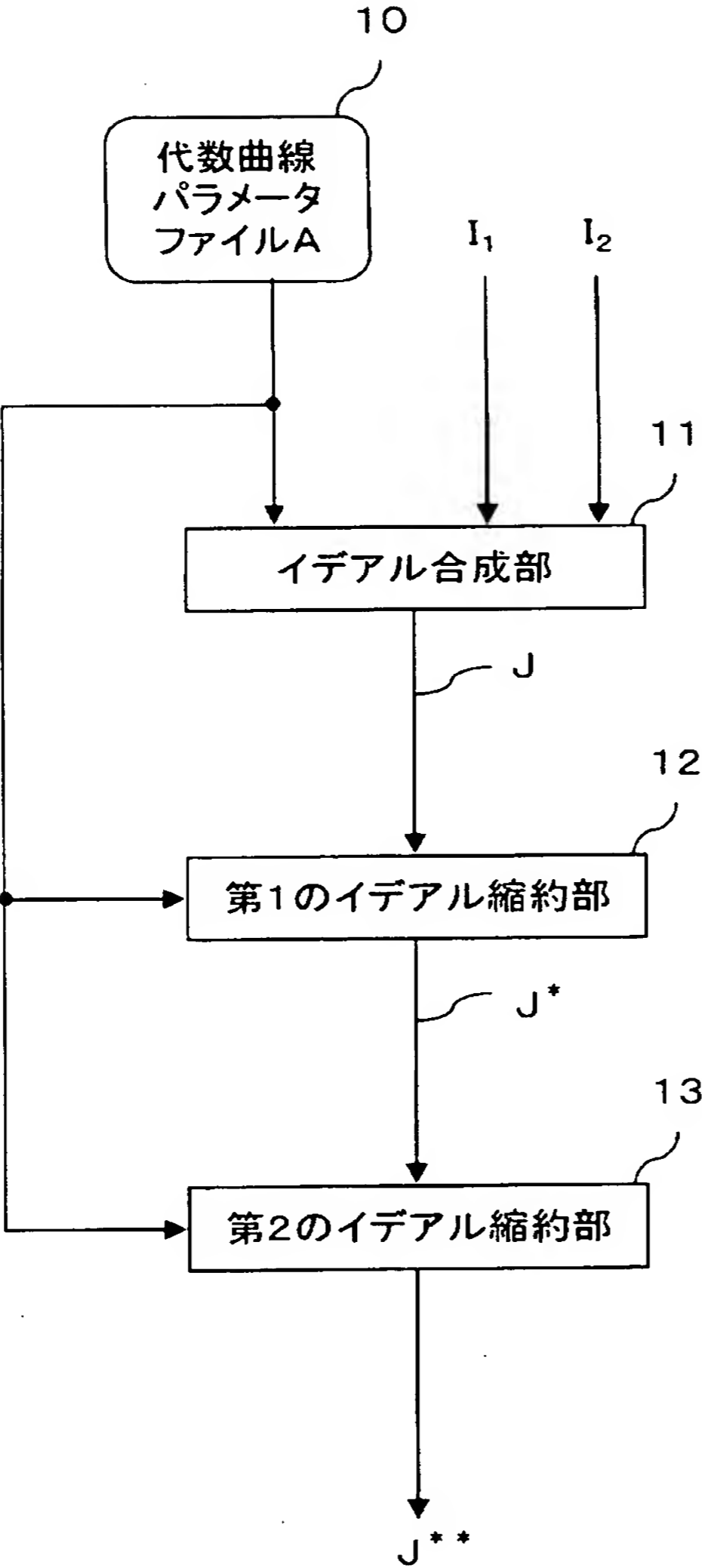
2 5, 3 5 イdeal型テーブル

2 6, 3 6 単項式リストテーブル

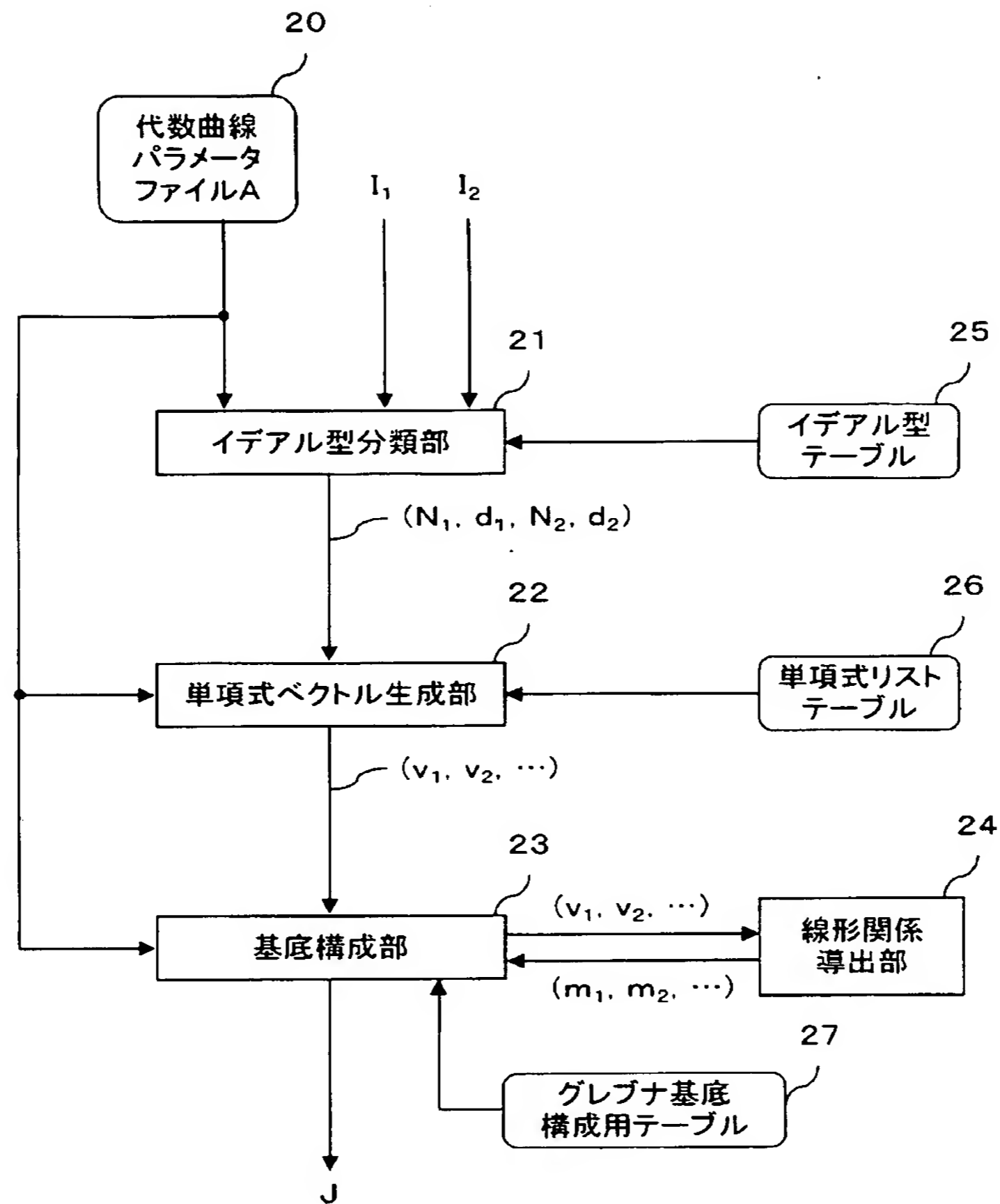
2 7, 3 7 グレブナ基底構成用テーブル

【書類名】 図面

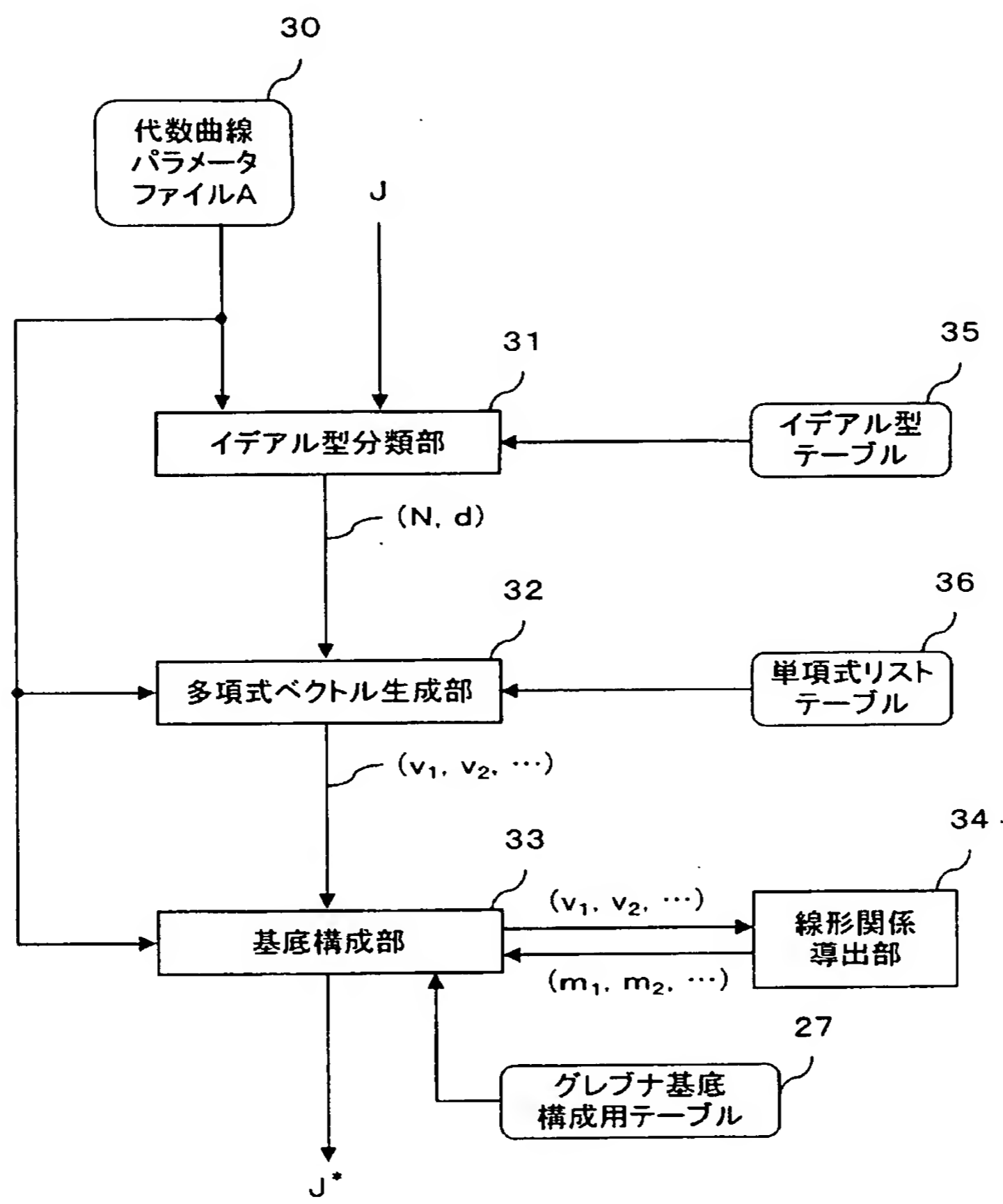
【図 1】



【図2】



【図 3】



【図 4】

定義体位数	1009
単項式順序	1, X, Y, X ² , X Y, Y ² , X ³ , X ² Y, X Y ² , X ⁴ , Y ³
係数リスト	0,7,0,0,0,0,0,0,0,1,1

【図5】

レコード番号	イデアル型番号	イデアル型	位数	縮約位数
1	61	$\{X^2 + a_4 Y^2 + a_5 XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^2 Y + b_4 Y^2 + b_5 XY + b_6 X^2 + b_3 Y + b_2 X + b_1, \\ XY^2 + c_4 Y^2 + c_5 XY + c_6 X^2 + c_3 Y + c_2 X + c_1\}$	6	3
2	62	$\{Y^2 + a_5 XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^3 + b_5 XY + b_6 X^2 + b_3 Y + b_2 X + b_1\}$	6	2
3	63	$\{Y^2 + a_5 XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^2 Y + b_6 X^3 + b_5 XY + b_4 X^2 + b_3 Y + b_2 X + b_1\}$	6	2
4	64	$\{XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^4 + b_6 X^3 + b_5 Y^2 + b_4 X^2 + b_3 Y + b_2 X + b_1\}$	6	1
5	65	$\{X^2 + a_3 Y + a_2 X + a_1\}$	6	0
6	51	$\{Y^2 + a_5 XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^3 + b_5 XY + b_6 X^2 + b_3 Y + b_2 X + b_1, \\ X^2 Y + c_5 XY + c_6 X^2 + c_3 Y + c_2 X + c_1\}$	5	3
7	52	$\{XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ Y^2 + b_6 X^2 + b_3 Y + b_2 X + b_1\}$	5	2
8	53	$\{XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ X^3 + b_5 Y^2 + b_6 X^2 + b_3 Y + b_2 X + b_1\}$	5	2
9	54	$\{X^2 + a_3 Y + a_2 X + a_1, \\ XY^2 + b_5 Y^2 + b_6 XY + b_3 Y + b_2 X + b_1\}$	5	1
10	41	$\{XY + a_6 X^2 + a_3 Y + a_2 X + a_1, \\ Y^2 + b_6 X^2 + b_3 Y + b_2 X + b_1, \\ X^3 + c_6 X^2 + c_3 Y + c_2 X + c_1\}$	4	3
11	42	$\{X^2 + a_3 Y + a_2 X + a_1, \\ XY + b_3 Y + b_2 X + b_1\}$	4	2
12	43	$\{X^2 + a_3 Y + a_2 X + a_1, \\ Y^2 + b_6 XY + b_3 Y + b_2 X + b_1\}$	4	2
13	44	$\{Y + a_2 X + a_1\}$	4	0
14	31	$\{X^2 + a_3 Y + a_2 X + a_1, \\ XY + b_3 Y + b_2 X + b_1, \\ Y^2 + c_3 Y + c_2 X + c_1\}$	3	3
15	32	$\{Y + a_2 X + a_1, X^3 + b_3 X^2 + b_2 X + b_1\}$	3	1
16	33	$\{X + a_1\}$	3	0
17	21	$\{Y + a_2 X + a_1, X^2 + b_2 X + b_1\}$	2	2
18	22	$\{X + a_1, Y^2 + b_2 Y + b_1\}$	2	1
19	11	$\{X + a_1, Y + b_1\}$	1	2

【図 6】

レコード番号	位数	単項式リスト
1	6	1, X, Y, X ² , X Y, Y ² , X ³ , X ² Y, X Y ² , X ⁴
2	5	1, X, Y, X ² , X Y, Y ² , X ³ , X ² Y, X Y ²
3	4	1, X, Y, X ² , X Y, Y ² , X ³
4	3	1, X, Y, X ² , X Y, Y ² , X ³
5	2	1, X, Y, X ² , X Y, Y ²
6	1	1, X, Y

【図 7】

レコード番号	位数	成分番号リスト	第一ベクトル型	第二ベクトル型	第三ベクトル型
1	6	7,8,9,10	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	(*,*,*,*,*,0,0,1,0)
2	6	6,7,9,10	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,1,0,0,0)	null
3	6	6,8,9,10	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,*,1,0,0)	null
4	6	5,8,9,10	(*,*,*,*,*,1,0,0,0,0,0)	(*,*,*,*,*,0,*,*,0,0,1)	null
5	6	4,7,8,10	(*,*,*,*,*,1,0,0,0,0,0,0)	null	null
6	5	6,7,8,9	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	(*,*,*,*,*,0,0,1,0)
7	5	5,6,8,9	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,1,0,0,0)	null
8	5	5,7,8,9	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,*,1,0,0)	null
9	5	4,7,8,9	(*,*,*,*,*,1,0,0,0,0,0)	(*,*,*,*,*,0,*,*,0,0,1)	null
10	4	5,6,7	(*,*,*,*,*,1,0,0)	(*,*,*,*,*,0,1,0)	(*,*,*,*,*,0,0,1)
11	4	4,5,7	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	null
12	4	4,6,7	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,*,1,0)	null
13	4	3,5,6	(*,*,*,*,*,1,0,0,0,0)	null	null
14	3	4,5,6,7	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	(*,*,*,*,*,0,0,1,0)
15	3	3,5,6,7	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,*,*,0,0,1)	null
16	3	2,4,5,7	(*,*,*,*,*,1,0,0,0,0,0)	null	null
17	2	3,4,5,6	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	null
18	2	2,4,5,6	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,*,*,0,0,1)	null
19	1	2,3	(*,*,*,*,*,1,0)	(*,*,*,*,*,0,1)	null

【図 8】

定義体位数	1009
単項式順序	1, X, X ² , X ³ , Y, X ⁴ , X Y, X ⁵ , X ² Y, X ⁶ , X ³ Y, X ⁷ , Y ²
係数リスト	0,7,0,0,0,0,0,0,0,0,1,1

【図 9】

レコード番号	イデアル型番号	イデアル型	位数	縮約位数
1	61	$\{X Y + a_6 X^4 + a_5 Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X^5 + b_6 X^4 + b_5 Y + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	6	3
2	62	$\{X^4 + a_5 Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X^2 Y + b_6 X Y + b_5 Y + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	6	2
3	63	$\{Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X^6 + b_6 X^5 + b_5 X^4 + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	6	1
4	64	$\{X^3 + a_3 X^2 + a_2 X + a_1\}$	6	0
5	51	$\{X^4 + a_5 Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X Y + b_5 Y + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	5	3
6	52	$\{Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X^5 + b_5 X^4 + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	5	2
7	53	$\{X^3 + a_3 X^2 + a_2 X + a_1, X^2 Y + b_5 X Y + b_4 Y + b_3 X^2 + b_2 X + b_1\}$	5	1
8	41	$\{Y + a_4 X^3 + a_3 X^2 + a_2 X + a_1, X^4 + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	4	3
9	42	$\{X^3 + a_3 X^2 + a_2 X + a_1, X Y + b_4 Y + b_3 X^2 + b_2 X + b_1\}$	4	2
10	43	$\{X^2 + a_2 X + a_1\}$	4	0
11	31	$\{X^3 + a_3 X^2 + a_2 X + a_1, Y + b_3 X^2 + b_2 X + b_1\}$	3	3
12	32	$\{X^2 + a_2 X + a_1, X Y + b_3 Y + b_2 X + b_1\}$	3	1
13	21	$\{X^2 + a_2 X + a_1, Y + b_2 X + b_1\}$	2	2
14	22	$\{X + a_1\}$	2	0
15	11	$\{X + a_1, Y + b_1\}$	1	1

【図 1 0】

レコード番号	位数	単項式リスト
1	6	1, X, X ² , X ³ , Y, X ⁴ , X Y, X ⁵ , X ² Y, X ⁶
2	5	1, X, X ² , X ³ , Y, X ⁴ , X Y, X ⁵ , X ² Y
3	4	1, X, X ² , X ³ , Y, X ⁴ , X Y
4	3	1, X, X ² , X ³ , Y, X ⁴ , X Y
5	2	1, X, X ² , X ³ , Y
6	1	1, X, X ² , X ³ , Y

【図 1 1】

レコード 番号	位 数	成分番号リ スト	第一ベクトル型	第二ベクトル型	第三ベク トル型
1	6	7,8,9,10	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	null
2	6	6,8,9,10	(*,*,*,*,*,1,0,0,0,0)	(*,*,*,*,*,0,*,0,1,0)	null
3	6	5,7,9,10	(*,*,*,*,1,0,0,0,0)	(*,*,*,*,0,*,0,*,0,1)	null
4	6	4,6,8,10	(*,*,*,1,0,0,0,0,0,0)	null	null
5	5	6,7,8,9	(*,*,*,*,*,1,0,0,0)	(*,*,*,*,*,0,1,0,0)	null
6	5	5,7,8,9	(*,*,*,*,1,0,0,0,0)	(*,*,*,*,0,*,0,1,0)	null
7	5	4,6,8,9	(*,*,*,1,0,0,0,0,0)	(*,*,*,0,*,0,*,0,1)	null
8	4	5,6,7	(*,*,*,*,1,0,0)	(*,*,*,*,0,1,0)	null
9	4	4,6,7	(*,*,*,1,0,0,0)	(*,*,*,0,*,1,0)	null
10	4	3,4,6	(*,*,1,0,0,0,0)	null	null
11	3	4,5,6,7	(*,*,*,1,0,0,0)	(*,*,*,0,1,0,0)	null
12	3	3,4,6,7	(*,*,1,0,0,0,0)	(*,*,0,0,*,0,1)	null
13	2	3,4,5	(*,*,1,0,0)	(*,*,0,0,1)	null
14	2	2,3,4	(*,1,0,0,0)	null	null
15	1	2,3,4,5	(*,1,0,0,0)	(*,0,0,0,1)	null

【図 1 2】

定義体位数	1009
単項式順序	1, X, X ² , Y, X ³ , XY, X ⁴ , X ² Y, X ⁵ , Y ²
係数リスト	0,7,0,0,0,0,0,0,1,1

【図 1 3】

レコード番 号	イデアル型 番号	イデアル型	位数	縮約位 数
1	41	$\{X^3 + a_4 Y + a_3 X^2 + a_2 X + a_1, \\ XY + b_4 Y + b_3 X^2 + b_2 X + b_1\}$	4	2
2	42	$\{Y + a_3 X^2 + a_2 X + a_1, \\ X^4 + b_4 X^3 + b_3 X^2 + b_2 X + b_1\}$	4	1
3	43	$\{X^2 + a_2 X + a_1\}$	4	0
4	31	$\{Y + a_3 X^2 + a_2 X + a_1, \\ X^3 + b_3 X^2 + b_2 X + b_1\}$	3	2
5	32	$\{X^2 + a_2 X + a_1, XY + b_3 Y + b_2 X + \\ b_1\}$	3	1
6	21	$\{X^2 + a_2 X + a_1, Y + b_2 X + b_1\}$	2	2
7	22	$\{X + a_1\}$	2	0
8	11	$\{X + a_1, Y + b_1\}$	1	1

【図 1 4】

レコード番号	位数	単項式リスト
1	4	1, X, X ² , Y, X ³ , X Y, X ⁴
2	3	1, X, X ² , Y, X ³ , X Y
3	2	1, X, X ² , Y
4	1	1, X, X ² , Y

【図 1 5】

レコード 番号	位数	成分番号 リスト	第一ベクトル型	第二ベクトル型	第三ベクトル型
1	4	5,6,7	(*,*,*,1,0,0)	(*,*,*,0,1,0)	null
2	4	4,6,7	(*,*,*,1,0,0,0)	(*,*,*,0,*,0,1)	null
3	4	3,5,7	(*,*,1,0,0,0,0)	null	null
4	3	4,5,6	(*,*,*,1,0,0)	(*,*,*,0,1,0)	null
5	3	3,5,6	(*,*,1,0,0,0)	(*,*,0,*,0,1)	null
6	2	3,4	(*,*,1,0)	(*,*,0,1)	null
7	2	2,3	(*,1,0,0)	null	null
8	1	2,3,4	(*,1,0,0)	(*,0,0,1)	null

【図 1 6】

	加算	2倍算
合成操作	134 M + 3 I	214 M + 3 I
タイプ 61 のイデアルに対する縮約操作	54 M + I	54 M + I
タイプ 31 のイデアルに対する縮約操作	16 M + I	16 M + I
合計	204 M + 5 I	284 M + 5 I

【書類名】 要約書

【要約】

【課題】 C_{ab} 曲線のヤコビ群における加算を高速に計算することができ、 C_{ab} 曲線の実用性を向上させることができるヤコビ群要素加算装置を得る。

【解決手段】 代数曲線パラメータファイル A 1 0 と、このファイル A で指定された代数曲線の座標環のイデアルのグレブナ基底 I_1 および I_2 とをイデアル合成部 1 1 へ入力し、イデアル積のグレブナ基底 J を演算する。第一のイデアル縮約部 1 2 で、ファイル A で指定された代数曲線の座標環における J が生成するイデアルの逆イデアルと同値のイデアルのうち、ファイル A で指定された単項式順序において最小のイデアルのグレブナ基底 J^* を演算する。第二のイデアル縮約部 1 3 で、この J^* が生成するイデアルの逆イデアルと同値のイデアルのうち、ファイル A で指定された単項式順序において最小のイデアルのグレブナ基底 J^{**} を演算して出力する。

【選択図】 図 1

特願 2 0 0 2 - 2 4 0 0 3 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1 . 変 更 年 月 日

1 9 9 0 年 8 月 2 9 日

[変 更 理 由]

新 規 登 録

住 所

東 京 都 港 区 芝 五 丁 目 7 番 1 号

氏 名

日 本 電 気 株 式 会 社